OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Securing the Revolution: An Academic Analysis of 5G Security, Zero Trust Architecture, and AI/ML Integration

Abass Abdelaziz Abass Kheder
Senior Communication Engineer Core Network consultant, Riyadh, Saudia Arabia

ABSTRACT: The fifth generation of mobile networks (5G) represents a paradigm shift in telecommunications, promising transformative capabilities through enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC). This evolution is underpinned by novel architectural constructs including Service-Based Architecture (SBA), However, these innovations concurrently introduce significant security and privacy challenges, expanding the threat landscape beyond that of previous generations. Vulnerabilities manifest in signaling protocols (HTTP/2, Diameter), susceptibility to sophisticated Distributed Denial of Service (DDoS) attacks, new forms of spoofing, and risks inherent in virtualization, shared resources via slicing, and distributed edge deployments. Traditional security models, often perimeter-based, prove insufficient for this dynamic, decentralized ecosystem. This article presents an in-depth academic analysis of the 5G architecture and its inherent security considerations, investigates the multifaceted threat landscape, and critically examines the application of Zero Trust Architecture (ZTA) and Artificial Intelligence/Machine Learning (AI/ML) as advanced mitigation strategies. Drawing upon established industry standards from organizations such as 3GPP, ETSI, and NIST, the analysis evaluates the principles, implementation models, benefits, and challenges associated with deploying ZTA and AI/ML in 5G environments. The findings indicate that a synergistic integration of ZTA principles, dynamically enforced and optimized through AI/ML capabilities, is essential for establishing a robust, adaptive, and privacy-preserving security framework capable of addressing the unique challenges of the 5G era.

KEYWORDS: 5G, Distributed Denial of Service, Machine Learning, smart city Saudi Arabia, Vision 2030.

Date of Submission: 13-05-2025 Date of acceptance: 27-05-2025

I. INTRODUCTION

Context: The 5G Transformation

Officially standardized by the International Telecommunication Union (ITU) as IMT-2020 and specified by the 3rd Generation Partnership Project (3GPP) starting from Release 15, the fifth generation of mobile telephony (5G) marks a revolutionary leap beyond its predecessors. Unlike incremental upgrades, 5G is designed as an end-to-end ecosystem enabling a fully mobile and connected society. It aims to deliver significantly improved services across several key dimensions: enhanced Mobile Broadband (eMBB) offering peak data rates exceeding 10 Gbps; Ultra-Reliable Low-Latency Communications (URLLC) targeting sub-millisecond latency for critical applications; and massive Machine-Type Communications (mMTC) supporting connection densities greater than 1 million devices per square kilometer. These capabilities are enabled by foundational technologies such as 5G New Radio (NR) operating across diverse spectrum bands (sub-1 GHz to mmWave), network slicing allowing customized virtual networks, and edge computing bringing processing closer to the user. Compared to 4G/LTE, 5G offers substantial performance gains, including potentially 100 times faster speeds, drastically

reduced latency (from ~50ms to <1ms), higher connection density, and improved spectrum efficiency. This technological advancement underpins a new wave of innovation, enabling diverse applications such as autonomous vehicles, smart cities, industrial IoT (IIoT), augmented/virtual reality (AR/VR), remote surgery, and advanced mobile broadband services.

The Security Imperative in 5G

The transformative potential of 5G is inextricably linked to the imperative of robust security and privacy. As 5G networks become foundational infrastructure for critical services across various sectors (healthcare, transportation, energy, manufacturing), the consequences of security breaches escalate dramatically. The expanded capabilities and novel use cases inherently increase the network's complexity and attack surface compared to 4G. The proliferation of connected devices, particularly in the massive IoT domain, introduces billions of potentially vulnerable endpoints. Furthermore, the shift towards software-based functions and open interfaces creates new avenues for exploitation. Protecting sensitive user data, ensuring service availability and integrity, and maintaining trust in the network are paramount for the successful adoption and societal benefit of 5G. The security challenges are not merely technical but also involve policy, regulation, and international cooperation.

Architectural Shifts and Security Implications

Central to 5G's capabilities are fundamental architectural shifts away from the more monolithic, hardware-centric designs of previous generations. Key enabling technologies include Network Function Virtualization (NFV), which runs network functions as software on standard hardware ; Software-Defined Networking (SDN), which separates the network control and data planes ; the Service-Based Architecture (SBA) in the 5G Core (5GC), which employs modular network functions communicating via APIs ; network slicing, which allows multiple logical networks to run on shared infrastructure ; and Multi-Access Edge Computing (MEC), which distributes computation towards the network edge. While these innovations provide unprecedented flexibility, scalability, and efficiency, they simultaneously introduce inherent security vulnerabilities. The reliance on software, virtualization, open interfaces, and shared resources fundamentally alters the security landscape, rendering traditional perimeter-based security models inadequate.

Emerging Security Paradigms: ZTA and AI/ML

Addressing the complex security challenges of 5G necessitates adopting advanced security paradigms. Zero Trust Architecture (ZTA), operating on the principle of "never trust, always verify," offers a response to the dissolution of traditional network perimeters. ZTA mandates continuous verification, least privilege access, and micro-segmentation, focusing security on resources and identities rather than network location. Concurrently, Artificial Intelligence (AI) and Machine Learning (ML) emerge as essential tools for managing the scale and complexity of 5G security. AI/ML enables advanced anomaly detection, automated threat intelligence analysis, and dynamic response mechanisms capable of handling the speed and sophistication of modern cyber threats.

Article Scope and Structure

This article provides a comprehensive academic analysis of 5G security and privacy, drawing upon established research and standardization efforts. It begins by detailing the 5G network architecture and the inherent security considerations arising from its foundational technologies (Section 2). Subsequently, it analyzes the multifaceted 5G threat landscape, identifying key vulnerabilities and attack vectors (Section 3). The article then explores the implementation of Zero Trust Architecture in 5G, examining its principles, application across the ecosystem, benefits, and challenges (Section 4). Following this, the role of AI/ML in enhancing 5G security through advanced detection and automated response is investigated (Section 5). Section 6 synthesizes these findings, discussing the synergistic relationship between ZTA and AI/ML in creating an adaptive security

framework, referencing relevant industry standards. Finally, Section 7 provides concluding remarks and outlines future research directions.

II. 5G Network Architecture and Inherent Security Considerations

Understanding 5G security requires a foundational grasp of its architecture, which differs significantly from previous generations and introduces unique security implications.

Architectural Overview

The 5G System (5GS) comprises three main components: the User Equipment (UE), the Next Generation Radio Access Network (NG-RAN), and the 5G Core Network (5GC).

- **User Equipment (UE):** Consists of the mobile station (e.g., smartphone, IoT device) and the Universal Subscriber Identity Module (USIM), which stores subscriber credentials.
- **Radio Access Network (NG-RAN):** The primary element is the gNodeB (gNB), the 5G base station supporting NR. The NG-RAN connects UEs to the 5GC, managing radio resources and handling wireless communication over various frequency bands (low, mid, high/mmWave) optimized for different coverage and capacity requirements. The NG-RAN architecture itself can be disaggregated into functions like the Centralized Unit (CU) and Distributed Unit (DU), facilitating flexible deployments and integration with edge computing. Initiatives like the O-RAN Alliance promote open interfaces within the RAN, aiming for greater vendor diversity but also introducing new security considerations related to these open interfaces and multi-vendor components.
- **5G Core Network (5GC):** The 5GC represents a fundamental departure from the 4G Evolved Packet Core (EPC). A key principle is the separation of Control Plane (CP) functions from User Plane (UP) functions, allowing independent scaling and deployment. The UP handles user data traffic, primarily managed by the User Plane Function (UPF). The CP manages signaling, authentication, session management, mobility, and policy control.

Service-Based Architecture (SBA): The 5GC CP employs a Service-Based Architecture (SBA), a significant shift from the point-to-point interfaces of 4G. In SBA, network capabilities are provided by modular software components called Network Functions (NFs). NFs act as service producers or consumers, interacting via well-defined Service-Based Interfaces (SBIs). These interactions typically use RESTful APIs over HTTP/2, secured by Transport Layer Security (TLS). This modular, software-driven approach enhances flexibility, scalability, reusability, and enables faster service innovation. Key NFs within the SBA include : * *Access and Mobility Management Function (AMF):* Manages UE registration, connection, reachability, and mobility. Acts as the primary CP contact point for the UE/RAN. * *Session Management Function (SMF):* Establishes, modifies, and releases UE PDU (Packet Data Unit) sessions, manages session context with UPF, allocates IP addresses. * *User Plane Function (UPF):* Routes and forwards user plane packets, performs packet inspection, enforces QoS, acts as the interconnect point to Data Networks (DN), and serves as a mobility anchor. * *Network Repository Function (NRF):* Supports service discovery, allowing NFs to discover and register available NF instances and their services. * *Network Exposure Function (NEF):* Securely exposes network capabilities and events to external third-party applications or internal NFs. * *Unified Data Management (UDM):* Manages user subscription data, generates authentication credentials, performs user identification, and supports authorization. May interact with a Unified Data Repository (UDR). * *Authentication Server Function (AUSF):* Performs authentication functions. * *Policy Control Function (PCF):* Provides a unified policy framework, managing policies for QoS, network behavior, and resource allocation. * *Network Slice Selection Function (NSSF):* Selects the appropriate network slice instance(s) for a UE. * *Service Communication Proxy (SCP):* Introduced in later releases, acts as an intermediary for NF communication, potentially simplifying routing and policy enforcement in complex deployments.

- **Multi-Access Edge Computing (MEC):** MEC involves deploying computing and storage resources at the edge of the network, typically close to the RAN or even at the enterprise premises. By processing data nearer to the end-user, MEC reduces end-to-end latency, decreases traffic load on the backhaul and core network, and enables context-aware, real-time applications like AR/VR, industrial automation,

autonomous systems, and content delivery networks. The European Telecommunications Standards Institute (ETSI) has been instrumental in standardizing MEC architectures and APIs.

Foundational Technologies Enabling 5G Architecture

Several key technologies underpin the 5G architecture and its capabilities:

- **Network Function Virtualization (NFV):** NFV decouples network functions (e.g., firewall, router, AMF, SMF) from dedicated hardware appliances. These functions are implemented as software, known as Virtual Network Functions (VNFs) or, in cloud-native contexts, Cloud-native Network Functions (CNFs), running on standard Commercial Off-The-Shelf (COTS) hardware, often within a cloud environment managed by NFV Management and Orchestration (MANO) systems. NFV provides agility, allowing NFs to be dynamically instantiated, scaled, and managed, reducing costs and accelerating service deployment.
- **Software-Defined Networking (SDN):** SDN separates the network's control plane from the data (forwarding) plane. A logically centralized SDN controller manages network behavior and traffic flows by programming the simpler data plane elements (switches/routers) via standardized interfaces (e.g., OpenFlow). This centralization enables network programmability, automated configuration, agile traffic management, and a global view of the network state.
- **Network Slicing:** A key 5G innovation, network slicing allows operators to partition the physical network infrastructure into multiple, isolated, end-to-end logical networks. Each slice can be customized with specific resources (compute, storage, network), functionalities, QoS parameters (bandwidth, latency, reliability), and security policies tailored to the needs of a particular service (e.g., high-bandwidth eMBB, low-latency URLLC, connection-dense mMTC) or customer group. Slices are identified by Single Network Slice Selection Assistance Information (S-NSSAI). This enables efficient resource utilization and supports diverse vertical industries with distinct requirements on a common infrastructure.
- **Massive IoT (mMTC):** 5G is designed to handle the massive connectivity demands of the Internet of Things, supporting significantly higher device densities than 4G. This involves optimizing the network for large numbers of devices that may transmit small amounts of data infrequently and require long battery life.

Emergent Security and Privacy Challenges

The architectural innovations and foundational technologies enabling 5G also introduce a complex array of new security and privacy challenges:

- **Increased Attack Surface:** The combination of virtualization, software-defined control, open APIs (SBIs), cloud deployment models (including edge), network slicing operating on shared infrastructure, and the massive influx of IoT devices dramatically expands the potential points of attack compared to previous, more contained network generations. Security perimeters become blurred or non-existent.
- **NFV/SDN Vulnerabilities:** Virtualization introduces risks associated with the hypervisor, VNF/CNF software vulnerabilities, insecure VNF lifecycle management, and potential interference between tenants sharing resources. The centralized NFV MANO and SDN controllers become high-value targets; compromising them could grant attackers extensive control over the network. Insecure southbound (controller-to-switch) and northbound (controller-to-application) interfaces can be exploited to manipulate traffic flows or inject malicious commands. Reliance on general-purpose OSs also imports known OS vulnerabilities.
- **SBA/HTTP/2 Risks:** The adoption of web technologies like HTTP/2 and REST APIs in the 5GC SBA, while promoting flexibility, also imports vulnerabilities common to web services into the critical core network infrastructure. This includes susceptibility to application-layer DoS attacks (e.g., exploiting stream multiplexing, slow-read tactics), API abuse, and potential vulnerabilities in the HTTP/2 protocol implementation itself. A compromised NF could leverage these protocols to attack other NFs.
- **Network Slicing Security Issues:** Ensuring robust isolation between network slices sharing the same physical infrastructure is paramount but challenging. Weak isolation can lead to cross-slice attacks, where a compromise in one slice affects another, enabling unauthorized access, data leakage, or resource consumption impacting slice performance guarantees (KPIs). Securing the slice lifecycle management processes (creation, modification, termination) and associated APIs is crucial to prevent unauthorized slice manipulation or resource theft. Protecting the confidentiality of slice identifiers (S-NSSAI) during transmission is also necessary.
- **Massive IoT Security Weaknesses:** Many IoT devices are resource-constrained (limited processing

power, battery) and may lack robust security features. Common issues include weak or default credentials, lack of secure update mechanisms, and insufficient encryption, making them easy targets for compromise. These compromised devices can form large-scale botnets used for DDoS attacks or serve as entry points for attackers to penetrate deeper into the network. Managing and securing such a vast and heterogeneous device population presents a significant challenge.

- **Edge Computing (MEC) Vulnerabilities:** Deploying network functions and applications at the edge introduces unique risks. Edge nodes may be located in environments with less physical security than centralized data centers, increasing vulnerability to tampering. Communication links (backhaul) connecting edge nodes to the core or management systems can be targeted. Shared edge infrastructure hosting third-party applications creates risks of interference or compromise if not properly isolated. Processing sensitive data at the edge also raises privacy concerns if security controls are inadequate. Vulnerabilities in MEC platforms or applications themselves can be exploited.
- **Privacy Concerns:** Despite improvements like SUCI, privacy risks remain. Location tracking might still be possible under certain conditions or through exploiting other signaling. The vast amount of data generated and processed, especially at the edge and within analytics functions like NWDAF, requires careful handling to prevent unauthorized access or leakage. Compromised NFs or edge nodes could potentially access sensitive subscriber information (e.g., SUPI, usage patterns). Ensuring privacy within shared slice or edge environments is also critical.

Security Posture Evolution from 4G/LTE

5G incorporates significant security enhancements compared to 4G/LTE, but also introduces new complexities and challenges.

- **Improvements:** 5G security architecture, particularly in Standalone (SA) mode, offers several advancements :
  - *Enhanced Authentication:* A flexible framework supporting Extensible Authentication Protocol (EAP) allows diverse credential types beyond USIMs (e.g., certificates, passwords), enabling integration with non-telecom systems. 5G Authentication and Key Agreement (5G-AKA) improves upon 4G's EPS-AKA. Mutual authentication is standard.
  - *Subscriber Privacy:* Encryption of the permanent subscriber identifier (SUPI) into a Subscription Concealed Identifier (SUCI) using the home network's public key significantly mitigates the threat of IMSI catchers and passive tracking over the air interface. Temporary identifiers (5G-GUTI) are used post-registration.
  - *Roaming Security:* The Security Edge Protection Proxy (SEPP) is introduced at the edge of each Public Land Mobile Network (PLMN) to secure control plane communication over the N32 interface between networks, providing authentication, integrity, and confidentiality for inter-PLMN signaling, addressing vulnerabilities in older protocols like SS7 and Diameter.
  - *Stronger Cryptography:* 5G mandates stronger encryption algorithms (e.g., AES, ZUC) and prohibits null integrity protection (except for emergency calls). User plane encryption is also supported.
  - *Native Slicing Security:* Security mechanisms are integrated into the network slicing framework, including slice-specific authentication/authorization (NSSAA) and NF authorization per slice.
  - *SBA Security:* The SBA design incorporates security principles, using TLS for securing SBIs and OAuth 2.0 for authorization between NFs.
- **Persistent/New Challenges:** Despite these improvements, significant challenges remain or are newly introduced by 5G's architecture:
  - *Legacy Protocol Interworking:* Roaming and interworking between 5G SA and older networks (4G/3G) still often rely on protocols like Diameter, inheriting their known vulnerabilities in these scenarios.
  - *Virtualization & Software Complexity:* The heavy reliance on NFV, SDN, and cloud-native principles introduces software vulnerabilities, configuration complexities, and risks associated with shared infrastructure, as discussed previously.
  - *Expanded Attack Surface:* The combination of IoT, edge computing, network slicing, and open interfaces creates a vastly larger and more complex attack surface to defend.
  - *IoT and Edge Security:** Securing billions of diverse, potentially resource-constrained IoT devices and managing security for distributed edge deployments remain major hurdles.

- *NSA Deployment Lag:* Early 5G Non-Standalone (NSA) deployments connect the 5G NR radio to the 4G EPC core. This configuration leverages existing infrastructure for faster rollout but inherits the security limitations and vulnerabilities of the 4G core. Many advanced 5G security features tied to the 5GC SA (e.g., full SBA security, SEPP, enhanced slicing security) are not available in NSA mode. Consequently, a significant security gap exists between the potential of 5G SA security and the reality of initial NSA deployments. The full security benefits are only realized upon migration to a complete 5G Standalone architecture.
- *Architectural Evolution as a Double-Edged Sword:* The very technologies that enable 5G's flexibility and performance—SBA, NFV, SDN, slicing, edge computing—are also the primary sources of its new security challenges. The shift from relatively static, hardware-based 4G networks to dynamic, distributed, software-centric 5G systems fundamentally increases the complexity of securing the infrastructure. Software vulnerabilities, insecure APIs, risks from shared resources, and the distribution of functions create numerous new potential weaknesses that require security to be deeply integrated into the design and operation, rather than being treated as an overlay.

Feature/Aspect	4G/LTE Description	5G SA Description	Key Differences/Improvements/Challenges
Core Architecture	Evolved Packet Core (EPC); Point-to-point interfaces; Hardware-centric NFs	5G Core (5GC); Service-Based Architecture (SBA); Cloud-native, virtualized NFs (VNFs/CNFs)	**Improvement:** Increased flexibility, scalability, agility. **Challenge:** Increased complexity, software vulnerabilities, API security risks.
Authentication	EPS-AKA; Primarily USIM-based	5G-AKA, EAP framework support (EAP-AKA', EAP-TLS); Allows diverse credentials	**Improvement:** More flexible and potentially stronger authentication options, support for non-3GPP access and vertical use cases.
User Privacy (ID)	IMSI transmitted less frequently but potentially exposed during initial procedures	SUPI (permanent ID) encrypted as SUCI using home network public key for transmission over air	**Improvement:** Significantly enhanced protection against IMSI catchers and passive tracking. **Challenge:** Residual risks (null-scheme, downgrade, SUCI-catchers).
Signaling Security	Diameter protocol for many core interfaces (e.g., AAA, policy)	HTTP/2 over TLS for SBIs within 5GC; RESTful APIs	**Improvement:** Aligns with modern web technologies, potentially better security if implemented correctly (TLS). **Challenge:** Imports web-based attack vectors (DoS, API abuse).
Roaming Security	Primarily Diameter and SS7 (MAP); Known vulnerabilities, often lacks E2E security	Security Edge Protection Proxy (SEPP) secures N32 interface between PLMNs using TLS/IPsec and application-level protection	**Improvement:** Dedicated security gateway (SEPP) provides enhanced inter-PLMN security compared to Diameter/SS7.
Network Slicing	Limited support (e.g., DECOR in later releases)	Native support; End-to-end logical networks with tailored characteristics; S-NSSAI identifier	**Improvement:** Enables diverse services on shared infrastructure. **Challenge:** Slice isolation, management security, cross-slice attacks.
Edge Computing	Limited concept/deployment	Integrated via Multi-Access Edge Computing (MEC); Standardized by ETSI	**Improvement:** Enables low-latency applications. **Challenge:** Physical security, shared infrastructure risks, MEC platform/app vulnerabilities.
Virtualization (NFV)	Introduced later in 4G lifecycle	Foundational; Core network designed for NFV/Cloud-native deployment	**Challenge:** Hypervisor/VNF vulnerabilities, MANO security, increased software attack surface.
Key Vulnerabilities	IMSI catching, Diameter attacks, Signaling (SS7)	SBA/HTTP/2 attacks, NFV/SDN vulnerabilities, Slice isolation	**Shift:** From protocol-specific (SS7/Diameter) and hardware-centric attacks towards

	exploits, EPC node vulnerabilities	failures, IoT botnets/DDoS, Edge security, SUCI tracking variants	software, API, virtualization, and large-scale distributed threats.

Table 1 : Comparative Analysis of Security Features and Challenges: 4G/LTE vs. 5G SA

III. Analysis of the 5G Threat Landscape

The architectural shifts in 5G create a complex and expanded threat landscape. Understanding the specific vulnerabilities and attack vectors across different domains is crucial for developing effective security strategies.

Signaling Plane Vulnerabilities and Attacks

The signaling plane, responsible for control functions like connection setup, mobility management, and authentication, is a critical target.

- **SBA and HTTP/2 Vulnerabilities:** The 5GC's reliance on SBA, with NFs communicating via RESTful APIs over HTTP/2 , introduces vulnerabilities typically associated with web services into the core network. Specific threats include :
  - *Denial of Service (DoS):* Exploiting HTTP/2 features like stream multiplexing (overwhelming an NF with many streams over one TCP connection) or slow-rate attacks (sending data slowly to tie up resources).
  - *API Abuse:* Malicious or compromised NFs/applications exploiting legitimate or poorly secured APIs (SBIs) to gain unauthorized access, extract sensitive information, or disrupt services.
  - *Compromised NF Attacks:* An attacker gaining control of one NF can use its legitimate SBI credentials to launch attacks against other NFs within the SBA. The need for sophisticated application-layer security and anomaly detection systems, beyond basic TLS encryption, becomes apparent to mitigate these risks. The Service Communication Proxy (SCP) can play a role in mediating these interactions and potentially enforcing policies.
- **Diameter Protocol Vulnerabilities (Roaming/Interworking):** While 5G SA utilizes SEPPs for enhanced inter-PLMN security using HTTP/2-based protocols , interaction with legacy 4G networks during roaming or migration phases often necessitates the use of the Diameter protocol. Diameter suffers from known security weaknesses, including :
  - *Lack of End-to-End Security:* Often deployed with hop-by-hop security or no credible security, especially when IPX providers (roaming brokers) are involved, leaving messages vulnerable in transit.
  - *Susceptibility to Attacks:* Vulnerable to spoofing, message tampering, information disclosure (e.g., subscriber location), DoS, and session hijacking. These vulnerabilities pose significant risks in roaming scenarios, potentially allowing attackers in one network to target subscribers or infrastructure in another. GSMA provides guidelines (FS.19, FS.21) to mitigate these risks, but the inherent weaknesses persist where Diameter is used.
- **Pre-authentication Message Exploits:** Even with 5G's security enhancements, messages exchanged between the UE and the network *before* full authentication and establishment of a security context remain vulnerable. These unprotected messages can potentially be intercepted or spoofed by attackers (e.g., using fake base stations) to launch DoS attacks against subscribers or glean sensitive information like location.
- **Replay Attacks:** Attackers may capture legitimate signaling messages and replay them later to cause disruption or gain unauthorized access. Potential targets include Non-Access Stratum (NAS) messages between the UE and AMF (over N1 interface), Packet Forwarding Control Protocol (PFCP) messages managing user plane tunnels, or network slice management commands. Proper sequence number checking, freshness mechanisms, and integrity protection are crucial mitigations.

Distributed Denial of Service (DDoS) Attack Vectors and Impacts

5G's architecture and scale create fertile ground for DDoS attacks.

- **Amplification via Massive IoT:** The mMTC use case connects billions of IoT devices. Many of these devices may have weak security, making them easily compromisable and recruitable into large-scale botnets. These botnets can then be leveraged to generate overwhelming traffic volumes for DDoS attacks, amplified by 5G's higher bandwidth capabilities.

- **Targeting Diverse Infrastructure:** DDoS attacks can target virtually any component of the 5G ecosystem:
  - *RAN:* Overloading gNBs with signaling or data traffic.
  - *Core Network:* Exhausting resources of critical NFs like AMF, SMF, UPF, or authentication servers (AUSF/UDM) through signaling floods or high-volume data traffic.
  - *Edge Computing (MEC):* Targeting MEC servers or applications to disrupt low-latency services.
  - *Network Slices:* Overwhelming the resources allocated to a specific slice, denying service to its users or applications.
  - *Signaling Plane:* Generating "signaling storms" (high rates of control messages) to overload control plane NFs.
- **Common Attack Types:** Techniques used include :
  - *Volumetric Attacks:* SYN Floods (exploiting TCP handshake), UDP Floods (sending large volumes of UDP packets, often fragmented), ICMP Floods.
  - *Protocol Attacks:* Exploiting weaknesses in protocols like TCP or DNS (e.g., DNS Floods targeting DNS infrastructure).
  - *Application Layer Attacks:* Targeting specific application protocols, such as HTTP/2 floods against SBA NFs. Newer patterns like short, high-intensity "pulse wave" attacks are also emerging, challenging detection systems.
- **Impact:** Successful DDoS attacks lead to service degradation or complete unavailability, network congestion, resource depletion in targeted components, poor Quality of Experience (QoE) for users, significant financial losses for operators, and damage to reputation. DDoS can also mask other malicious activities like data theft or malware insertion.

Spoofing Threats

Spoofing involves impersonating a legitimate entity (user, device, network function) to deceive systems or gain unauthorized access.

- **Identity Spoofing (SUPI/SUCI):** While SUCI encryption is a major improvement over exposing IMSI, residual risks allow for potential identity tracking or spoofing:
  - *Null-Scheme Usage:* If the home network hasn't provisioned its public key or explicitly configures the "null-scheme," the UE might send the SUPI in plaintext, making it vulnerable like IMSI.
  - *Downgrade Attacks:* Attackers might force a UE to connect to a legacy network (4G/3G/2G) where IMSI exposure risks are higher.
  - *SUCI Catchers/Crackers:* Even with encryption, attackers might track users by observing SUCI transmissions or attempt to link a specific SUCI back to a known SUPI/IMSI by probing or exploiting aspects of the authentication (AKA) procedure.
  - *API-Based SUPI Retrieval:* An adversary controlling a malicious or compromised Application Function (AF) or Network Function (NF) could potentially query the NEF or UDM using a known public identifier (like a phone number/GPSI) to retrieve the corresponding SUPI via legitimate SBA APIs (e.g., Nnef_ApplyPolicy_Create or Nudm_SDM_Get). This bypasses air interface protections.
- **Base Station (gNB) Spoofing:** Attackers can deploy fake base stations (rogue gNBs) by exploiting the fact that initial System Information Blocks (SIBs, carried in SSBs) broadcast by gNBs are unauthenticated and unencrypted. By transmitting a stronger signal than legitimate gNBs, a fake station can lure UEs to connect to it. Once connected, the rogue gNB can launch various attacks:
  - *Denial of Service (DoS):* Preventing UEs from accessing legitimate services.
  - *Downgrade Attacks:* Forcing UEs onto less secure 2G/3G/4G networks.
  - *Information Leakage:* Capturing sensitive information, potentially including IMSI/SUPI if null-scheme is used or through downgrade attacks.
  - *Location Tracking:* Identifying the presence and location of specific UEs.
  - *Man-in-the-Middle (MiTM):* Intercepting and potentially modifying user traffic if further security measures are bypassed.
  - *Signaling Manipulation:* Techniques like the "SigUnder" attack involve transmitting carefully crafted signals to overwrite specific bits in the legitimate gNB's Master Information Block (MIB) within the SSB, potentially barring UEs from the cell or disrupting handovers. Detection and

mitigation are challenging due to the lack of initial authentication. GNSS spoofing can also indirectly impact gNB operations by falsifying timing or location data, though 5G signals themselves might aid in detecting such GNSS attacks. Hardware modifications or counterfeit components in gNBs also pose a spoofing-related risk.

- **Network Function (NF) Spoofing:** Within the SBA, a compromised or rogue NF could potentially impersonate another legitimate NF. By spoofing the identity of a trusted NF, an attacker could intercept sensitive signaling messages, inject malicious commands, access restricted data (e.g., a rogue AMF querying the SMF for UE session context, including SUPI and slice information), or disrupt core network operations. If protocols like SCTP are used for transport between NFs, vulnerabilities like SCTP hijacking (e.g., using spoofed ABORT chunks) could also be exploited to disrupt connections or potentially impersonate endpoints.

Risks Associated with Network Slicing and Edge Computing

These key 5G enablers introduce specific vulnerabilities.

- **Network Slicing Vulnerabilities:**
  - *Cross-Slice Attacks:* This is a major concern. If the logical isolation between slices sharing the same physical infrastructure (compute, network, storage) is insufficient, vulnerabilities or compromises in one slice could potentially be exploited to access data, disrupt services, or consume resources belonging to another slice. Attack vectors could include exploiting shared resource vulnerabilities (e.g., hypervisor) or misconfigurations in slice boundaries or inter-slice communication policies.
  - *Slice Management Attacks:* The functions responsible for managing the lifecycle of network slices (e.g., creation, configuration, termination) and their associated APIs are potential targets. Attackers might attempt to hijack permissions, tamper with slice requests or Network Slice Templates (NSTs), leading to malicious slice creation, resource allocation confusion, information leakage, or DoS against the management plane.
  - *Resource Exhaustion/Theft:* An unauthorized UE gaining access to a slice, or a compromised slice itself, could consume excessive resources (bandwidth, compute), impacting the performance and availability of that slice or potentially other slices sharing the infrastructure.
  - *Data Leakage/Contamination:* Sensitive data could leak between slices if isolation mechanisms fail, or data could be contaminated if one slice can write to resources accessible by another.
  - *URSP Exploitation:* The User Equipment Route Selection Policy (URSP) mechanism allows UEs/applications to influence slice selection. Malware on a UE could potentially abuse URSP rules to request access to inappropriate slices or use slice access as an attack vector.
- **Edge Computing (MEC) Vulnerabilities:**
  - *Physical Security:* Edge nodes are often deployed outside secure central data centers (e.g., at base station sites, enterprise premises), making them more susceptible to physical tampering, theft, or unauthorized access.
  - *Insecure Communications:* Backhaul links connecting edge nodes to the core network, or management links used for orchestration, may traverse less trusted networks and require strong security (e.g., SecGW for backhaul) to prevent eavesdropping or MiTM attacks.
  - *Shared Infrastructure Risks:* MEC environments often host applications from multiple tenants or third parties on shared hardware and platform resources. This creates risks of interference, resource contention, or security breaches spreading between applications if isolation (e.g., via VNFs, containers, micro-segmentation) is inadequate.
  - *API and Application Security:* APIs exposed by the MEC platform or applications running on it can be vulnerable to attack if not properly secured. Third-party applications deployed at the edge might contain vulnerabilities or malicious code.
  - *Data Security at the Edge:* Processing and potentially storing sensitive data closer to users at the edge raises concerns about data confidentiality and integrity, especially if the edge environment itself is less secure than the core.
  - *Compromised Edge Nodes:* An attacker gaining control of an edge node could intercept local user traffic, manipulate edge applications, use the node as a launchpad for attacks against the core network or other UEs, or disrupt critical low-latency services.

The interconnected nature of these threats is significant. A vulnerability in one area, such as a poorly secured IoT device, can be exploited to launch an attack on another part of the system, like a network slice or an edge server. For instance, compromised IoT devices forming a botnet could execute a DDoS attack targeting a specific network slice's resources or disrupt an edge application. Similarly, a signaling attack might disable a security function, paving the way for a subsequent spoofing or data exfiltration attempt. This highlights the inadequacy of siloed security approaches; defenses must be holistic and capable of correlating events across different domains (RAN, Core, Edge, Slice, IoT).

Furthermore, many of these diverse threats converge on the fundamental challenge of Identity and Access Management (IAM). Whether it's UE authentication (SUPI/SUCI), NF interactions in the SBA, slice access control, or securing MEC platforms and management interfaces, verifying identity and enforcing appropriate authorization are central to mitigating risk. Spoofing directly targets identity verification, DDoS often obscures attacker identity, signaling attacks aim to bypass authentication, and slicing/edge attacks frequently involve unauthorized access. This underscores the critical need for robust, granular, and continuously enforced IAM across all entities and resources in the 5G ecosystem, naturally leading to considerations of architectures like Zero Trust.

Threat Category	Specific Threat Vector	Potential Targets	Primary Impact	Relevant Snippets
Signaling Attacks	HTTP/2 Stream Multiplexing/Slow Rate DoS	SBA NFs (AMF, SMF, PCF, etc.)	DoS, Resource Exhaustion	
	SBA API Abuse / Unauthorized Access	SBA NFs, NEF, UDM	Information Disclosure, Unauthorized Access, Service Disruption	
	Diameter Protocol Exploits (Roaming/Interworking)	Roaming Interfaces, EPC/5GC Interworking Functions, Partner Networks	DoS, Information Disclosure (Location), Spoofing, MiTM	
	Pre-authentication Message Exploits	UE, Initial Access Procedures	DoS, Information Disclosure (Location)	
	Signaling Message Replay (NAS, PFCP, Slice Mgmt)	AMF, SMF, UPF, Slice Management NFs	DoS, MiTM, Unauthorized Slice Modification	
DDoS Attacks	Volumetric Floods (SYN, UDP, ICMP) via IoT Botnets	RAN (gNBs), Core NFs (UPF, AMF), Edge Servers, Specific Slices/Services	Service Unavailability, Network Congestion, Resource Exhaustion	
	Application Layer DDoS (e.g., HTTP/2)	SBA NFs	Service Unavailability, Resource Exhaustion	
	Signaling Storms	Core NFs (AMF, SMF)	Control Plane Overload, Service Unavailability	
Spoofing Threats	SUPI/SUCI Tracking/Retrieval (Null-Scheme, API, Catcher)	UE Identity/Privacy	Location Tracking, User Identification, Enabling Further Attacks	
	Base Station (gNB) Spoofing (e.g., SigUnder)	UE Connection, RAN	DoS, MiTM, Information Leakage, Downgrade Attack	
	Network Function (NF) Spoofing	SBA NFs, Core Network Operations	Unauthorized Access, Data Manipulation, Service Disruption, MiTM	
Slicing Attacks	Cross-Slice Attacks (Weak Isolation)	Network Slice Instances, Shared Infrastructure	Unauthorized Access, Data Leakage, Performance Impact on Other Slices	

	Slice Management Interface Attacks	Slice Management NFs (CSMF, NSMF), Slice Lifecycle	Malicious Slice Creation/Modification, Resource Theft, DoS	
	Slice Resource Exhaustion	Network Slice Resources	DoS for Slice Users, Impact on Slice KPIs	
Edge (MEC) Attacks	Physical Tampering	Edge Nodes/Servers	Data Theft, Service Disruption, Node Compromise	
	Insecure Backhaul/Management Links	Edge Connectivity	Eavesdropping, MiTM, Unauthorized Management Access	
	Compromise of Shared Edge Infrastructure/Apps	MEC Platform, MEC Applications, Other Tenants	Data Leakage, Lateral Movement, Service Disruption	
Virtualization Attacks	Hypervisor Escape / Vulnerabilities	NFVI (NFV Infrastructure), Host OS	Unauthorized Hardware Access, VM Manipulation, Cross-Tenant Attacks	
	VNF/CNF Software Vulnerabilities	Specific Network Functions	NF Compromise, Service Disruption, Data Leakage	
	SDN Controller Compromise	Network Control Plane	Loss of Network Control, Traffic Manipulation, Widespread DoS	
	MANO System Compromise	VNF Lifecycle Management	Unauthorized VNF Deployment/Modification, Resource Manipulation	

Table 2 : Taxonomy of 5G Threat Vectors and Potential Targets

IV. Implementing Zero Trust Architecture (ZTA) in 5G Networks

Given the limitations of traditional security models and the expanded, complex threat landscape of 5G, Zero Trust Architecture (ZTA) emerges as a compelling security philosophy and architectural approach.

Foundational Principles and Logical Components of ZTA (Based on NIST SP 800-207)

ZTA fundamentally shifts the security posture from implicit trust based on network location to explicit verification for every access attempt.

- **Core Philosophy:** The central tenet is "Never trust, always verify". ZTA assumes no implicit trust is granted to users, devices, or network components merely because they are inside a perceived network perimeter. Instead, it focuses on protecting resources (data, applications, services, assets) directly. It operates with an "assume breach" mentality, meaning defenses are designed with the expectation that attackers may already be present within the network.
- **NIST SP 800-207 Tenets:** The US National Institute of Standards and Technology (NIST) Special Publication 800-207 provides widely recognized guidance on ZTA. Its seven core tenets are :
    1. All data sources and computing services are considered resources.
    2. All communication is secured regardless of network location.
    3. Access to individual enterprise resources is granted on a per-session basis.
    4. Access to resources is determined by dynamic policy (based on identity, device posture, context, etc.).
    5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
    6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
    7. The enterprise collects as much information as possible about assets, network infrastructure, and communications and uses it to improve its security posture.
- **Logical Components:** NIST SP 800-207 defines a logical architecture with key components responsible for mediating access :

  - Policy Engine (PE): The decision-making component. It evaluates access requests based on enterprise policies and various inputs (e.g., identity verification, device posture, threat intelligence, context) using a trust algorithm to grant or deny access.
  - Policy Administrator (PA): Responsible for establishing or terminating the communication path based on the PE's decision. It instructs the Policy Enforcement Point (PEP) and may generate session-specific credentials.
  - Policy Enforcement Point (PEP): The component that actually enables, monitors, and terminates connections between a subject (user, device, service) and a resource. It enforces the decisions made by the PE/PA. PEPs can be implemented as agents on clients/servers or as network gateways. The area behind the PEP containing the protected resource is sometimes referred to as the Implicit Trust Zone, though trust is still explicitly managed per session. The PE relies on various data sources like Continuous Diagnostics and Mitigation (CDM) systems, threat intelligence feeds, Identity Management systems, Security Information and Event Management (SIEM) systems, and defined data access policies to make informed decisions.
- **Key Enabling Concepts:** Implementing ZTA relies on several supporting security concepts and technologies:
  - Least Privilege Access (LPA): Granting users, devices, and applications only the minimum permissions necessary to perform their required tasks for the minimum time required.
  - Micro-segmentation: Dividing the network into small, isolated segments or zones, often down to the individual workload or application level, with strict access controls enforced between segments. This limits lateral movement for attackers.
  - Strong Authentication / Multi-Factor Authentication (MFA): Rigorously verifying the identity of users and devices before granting any access, often requiring multiple forms of evidence.
  - Continuous Monitoring and Validation: Constantly monitoring network traffic, user behavior, and device health to detect anomalies, reassess trust, and dynamically adjust access rights.
  - Identity and Access Management (IAM): Comprehensive systems for managing identities (user, device, service), credentials, and access policies.

Application of ZTA Across the 5G Ecosystem

To be effective, ZTA principles must be applied holistically across the entire 5G ecosystem, not just at the network edge. This involves securing interactions between and within all major components.

- **User Equipment (UE) Access:** ZTA extends beyond initial network authentication (like 5G-AKA). It involves continuously verifying the UE's identity and security posture (device health, software integrity) and authorizing access to specific services, applications, or network slices based on dynamic policies and user context. LPA should be applied to UE permissions.
- **Radio Access Network (RAN):** In traditional RANs, ZTA involves securing communication between gNB components (e.g., CU-DU F1 interface) and between the RAN and the Core. In Open RAN (O-RAN) architectures, ZTA is crucial for securing the open interfaces (e.g., Fronthaul, X2/Xn-like interfaces) and interactions between disaggregated components (O-RU, O-DU, O-CU) and the SMO/RIC platforms. Access to RAN management functions and APIs must be strictly controlled based on ZTA principles. In scenarios with intermittent backhaul connectivity (e.g., tactical networks), delegating certain ZTA decision-making or enforcement capabilities (like cached decisions or replicated logic) to the RAN (potentially via RIC xApps) might be necessary.
- **Core Network (SBA):** ZTA principles are highly relevant to the SBA. Each NF acts as both a subject requesting services and a resource providing services. Communication via SBIs must be secured through strong mutual authentication (e.g., using certificates managed by a PKI) and fine-grained, dynamic authorization based on policy. Authorization should verify that the consuming NF is permitted to access the specific service offered by the producing NF, potentially on a per-slice basis. Enforcement could occur at the NFs themselves, or via intermediaries like Service Communication Proxies (SCPs) or sidecar proxies deployed alongside NFs. The integrity and security posture of each NF instance should also be continuously assessed.
- **Edge Computing (MEC):** ZTA is essential for securing the distributed MEC environment. This includes securing the MEC platform itself, authenticating and authorizing MEC applications before allowing them to run or access platform services/APIs, securing communication between MEC applications and between MEC and the Core/RAN, and applying micro-segmentation to isolate applications and tenants running on

shared edge infrastructure. Device posture checks should apply to MEC hosts.

- **Network Slicing:** ZTA principles directly support network slicing security requirements. Micro-segmentation is the core mechanism for enforcing isolation between slices. Dynamic, policy-based access control should govern UE access to specific slices (based on subscription, context, S-NSSAI) and inter-slice communication where permitted. NF authorization within the SBA should be slice-specific. ZTA must also secure the slice management and orchestration functions.
- **Management and Orchestration (M&O):** Access to critical M&O systems (e.g., NFV MANO, O-RAN SMO, Core Network management) by human administrators or automated systems must be governed by ZTA. This involves strong authentication (MFA), strict LPA, and continuous monitoring of management activities.

ZTA Principle (NIST SP 800-207 Tenet)	UE Application	RAN Application	Core (SBA) Application	Edge (MEC) Application	Network Slice Application	Management Application
1. All Resources Identified	UE treated as resource endpoint	gNBs, CUs, DUs, O-RAN components (O-RU/DU/CU, RIC) identified as resources	Each NF instance (AMF, SMF, UPF, NRF, etc.) treated as a resource	MEC Host, MEC Platform, MEC Applications identified as resources	Each Network Slice Instance (NSI) and its constituent NFs treated as resources	MANO, SMO, Element Managers, Policy Servers identified as resources
2. Secure All Communication	Encrypted communication over radio (AS/NAS Security); Secure comms to MEC/Apps	Secure interfaces (e.g., F1, E1, Xn, O-RAN interfaces); Secure backhaul to Core (e.g., via SecGW)	Mutual TLS for SBIs; End-to-end encryption where applicable; SEPP for inter-PLMN N32 interface	Secure APIs; Encrypted communication between MEC Apps, MEC Platform, Core, and RAN; Secure VNF/CNF communication	Secure communication within slice NFs; Secure inter-slice communication (if allowed); Encrypted user plane traffic	Secure protocols (e.g., HTTPS, SSH) for management access; Encrypted communication between M&O components
3. Per-Session Access	Access to specific services/slices granted per session based on verification	Access between RAN components or to Core granted per session; Resource allocation based on session needs	NF-to-NF service requests authorized per session; Session context established/released by SMF	MEC application access to platform services or network info granted per session; Compute/storage resources allocated per session	UE access to slice resources granted per session; Resources within slice allocated based on session requirements	Administrator/system access to management functions granted per session
4. Dynamic Policy-Based Access	Access policies consider UE identity, device posture, location, time, requested service/slice	Policies control RAN resource allocation, handovers, connection to Core based on UE context, network load	SBI access policies based on consuming/producing NF identity, required service, slice context, security posture	Policies govern MEC app deployment, resource usage, API access based on app identity, tenant, security requirements	Slice access policies based on UE subscription (S-NSSAI), context, slice KPIs; Policies govern resource allocation within slice	Access policies based on role (RBAC), context, time for management tasks; Automated policy updates

						based on network state
5. Monitor Asset Integrity/Posture	Continuous UE device health/compliance checks (e.g., via MDM/agent)	Monitoring gNB/O-RAN component integrity, software versions, configuration compliance	Monitoring NF instance health, resource usage, software integrity, vulnerability status	Monitoring MEC host integrity, platform health, application behavior, resource consumption	Monitoring health and performance of slice NFs; Ensuring slice isolation integrity	Monitoring M&O system integrity, configuration changes, logs
6. Dynamic AuthN/AuthZ Enforcement	Re-authentication/authorization based on context changes or policy	Continuous verification of RAN component identities and authorization for interactions	Ongoing validation of NF credentials/tokens for SBI access; Dynamic authorization updates via PA/PEP	Continuous verification of MEC app identity/permissions; Dynamic enforcement of access policies at MEC platform/gateway	Continuous enforcement of slice access policies; Re-validation for inter-slice interactions	Dynamic enforcement of management access controls; Re-authentication for privileged operations
7. Collect Info for Posture Improvement	Collect UE connection logs, security events, device posture data	Collect RAN performance data, security logs, interface traffic statistics	Collect NF interaction logs, performance metrics, security alerts (e.g., via SIEM, NWDAF)	Collect MEC platform logs, application performance/security data, resource utilization metrics	Collect slice performance KPIs, resource usage data, security events within the slice	Collect management access logs, system performance data, configuration audit trails

Table 3 : Mapping ZTA Principles to 5G Ecosystem Components

ZTA Implementation Models and Standardization

Implementing ZTA in 5G involves leveraging existing standards and frameworks while adapting ZTA concepts to the telecom environment.

- **NIST SP 800-207 as Foundation:** NIST's framework provides the core principles and logical components (PE, PA, PEP) that guide ZTA implementation, although it's a conceptual model, not a specific telecom standard. Organizations adapt these concepts to their specific context.
- **3GPP Security as Enablers:** While 3GPP specifications (like TS 33.501 for security architecture) do not explicitly define a ZTA, they provide crucial building blocks that *enable* or *support* a ZTA implementation. These include:
    - Strong authentication mechanisms (5G-AKA, EAP support).
    - User identity protection (SUCI).
    - Secure interfaces (NAS/AS protection, TLS/OAuth for SBIs).
    - Roaming security (SEPP).
    - Network slicing security features (NSSAA, NF authorization per slice). Operators build their ZTA upon these standardized features. Ongoing 3GPP work in areas like enhanced slice security continues to evolve relevant capabilities.
- **ETSI Standards:** ETSI contributes standards relevant to specific domains within a 5G ZTA. ETSI ISG MEC defines architectures and APIs for the edge, including security considerations. ETSI ISG NFV provides specifications for securing the virtualized infrastructure (NFVI) and VNFs. ETSI TC CYBER works on broader cybersecurity standards applicable to telecom.
- **O-RAN Alliance:** Recognizing the security challenges of its open, multi-vendor architecture, the O-RAN Alliance is actively incorporating ZTA principles into its security specifications to protect interfaces and

components within the Open RAN ecosystem.

- **Implementation Models:** ZTA is not a single product but an architectural approach. Implementation often involves integrating multiple vendor solutions. Models can be identity-centric (focusing on user/device verification), network-centric (focusing on micro-segmentation and traffic control), or application/workload-centric. A comprehensive 5G ZTA likely requires elements of all three. The concept of an "intelligent ZTA" (i-ZTA) proposes leveraging AI/ML integrated with architectures like O-RAN to enable more dynamic, real-time trust evaluation and policy enforcement, moving beyond static rules.

Evaluation of ZTA in 5G: Benefits vs. Challenges

Deploying ZTA in 5G networks offers significant potential benefits but also presents considerable challenges.

- **Benefits:**
  - Enhanced Security Posture: Fundamentally improves security by eliminating implicit trust, reducing the attack surface, and making it harder for attackers to gain initial access and move laterally within the network.
  - Improved Threat Detection & Response: Continuous monitoring and verification enable faster detection of anomalies and breaches, facilitating quicker response and containment.
  - Better Data Protection: Focuses protection directly on resources and data, regardless of location (core, edge, cloud).
  - Increased Resilience: Micro-segmentation limits the "blast radius" of breaches, isolating compromised areas and allowing other parts of the network to continue operating.
  - Compliance Enablement: Helps meet stringent regulatory and internal security/privacy requirements.
  - Support for Modern Architectures: Well-suited for securing complex, distributed environments involving cloud, edge computing, remote access, and IoT.
  - Simplified Auditing: Granular logging of access decisions provides clear audit trails.
  - Business Enablement: Provides the necessary security foundation for advanced 5G services like secure network slicing for verticals and trusted edge applications, potentially unlocking new revenue streams. By enhancing trust, ZTA can encourage enterprise adoption of private 5G and mission-critical services.
- **Challenges:**
  - Implementation Complexity: Integrating ZTA across the diverse and complex components of a 5G network (RAN, Core SBA, Edge, Slices, M&O) involving multiple vendors and technologies (NFV, SDN) is a significant undertaking. It requires careful planning, robust policy definition, and phased deployment over multiple years.
  - Performance Impact: The overhead associated with continuous verification, encryption/decryption, policy lookups, and communication with PE/PA components for every session can potentially introduce latency and impact throughput. This is a critical concern for latency-sensitive URLLC services. Balancing the stringency of ZTA controls with 5G performance requirements is a key challenge.
  - Interoperability: Achieving seamless interoperability between ZTA components (PE, PA, PEP) from different vendors, and integrating them with existing 5G network functions and legacy systems, can be difficult due to the lack of fully standardized telecom-specific ZTA interfaces.
  - Scalability: The sheer scale of 5G—billions of devices, massive numbers of sessions, high data rates—poses a significant challenge for scaling the ZTA control plane (PE/PA) and enforcement mechanisms (PEPs) to handle the load without becoming bottlenecks.
  - Policy Management Complexity: Defining, managing, and dynamically updating the fine-grained access policies required for ZTA across the entire ecosystem is complex and requires sophisticated tools and processes.
  - Legacy Integration: Transitioning from existing security architectures and integrating ZTA principles with legacy systems during the migration from 4G to 5G SA presents practical difficulties.
  - Cost and Resources: Implementing ZTA requires investment in new security technologies, integration efforts, and potentially retraining personnel.

The inherent tension between ZTA's "always verify" mandate and the performance/complexity demands of 5G is evident. Every verification step adds potential latency and processing load, while managing the distributed enforcement and dynamic policies increases operational complexity. This tension highlights why a naive ZTA implementation might be impractical or detrimental in some 5G scenarios. Successfully deploying ZTA in 5G necessitates careful architectural design, optimization, and significant automation. This naturally leads to the exploration of AI and ML as critical enablers to manage the complexity, perform real-time analysis, and automate enforcement, thereby making ZTA feasible at 5G scale and speed.

V. Leveraging Artificial Intelligence and Machine Learning (AI/ML) for 5G Security

The dynamism, scale, and complexity of 5G networks, coupled with the increasing sophistication of cyber threats, make AI and ML indispensable tools for achieving robust security.

AI/ML-Powered Anomaly Detection and Threat Identification

Traditional security methods, often relying on predefined signatures or static rules, struggle to keep pace with the evolving threat landscape and the sheer volume of data in 5G. AI/ML offers the ability to learn complex patterns, adapt to changing conditions, and detect previously unseen (zero-day) threats.

- **Anomaly Detection:** ML and Deep Learning (DL) algorithms can establish baselines of normal network behavior and identify statistically significant deviations that may indicate malicious activity or network faults. Various algorithms have been explored, including supervised methods like K-Nearest Neighbors (KNN), Decision Trees (DT), Support Vector Machines (SVM), Random Forests (RF), Gradient Boosting (GB), and Logistic Regression (LR), as well as unsupervised methods like Autoencoders, and DL architectures like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) variants (LSTM, BiLSTM), and Transformers (BERT). Ensemble methods, like Voting Classifiers combining multiple models, often show strong performance. The goal is high accuracy in detecting threats while minimizing false positives, which can overwhelm security teams.
- **Specific Use Cases:** AI/ML is being applied to detect various 5G threats:
    - *SBA Security:* Detecting anomalous HTTP/2 traffic patterns between NFs indicative of DoS attacks or API abuse.
    - *Signaling DDoS:* Identifying signaling storms or coordinated malicious signaling targeting core NFs (AMF, SMF).
    - *Intrusion Detection:* General intrusion detection within the 5G core, RAN, or specific network slices.
    - *IoT Security:* Detecting compromised IoT devices based on abnormal communication patterns or participation in botnet activities.
    - *Application-Specific Security:* Detecting attacks in 5G-enabled applications like smart grids.
- **Encrypted Traffic Analysis:** A significant challenge in modern networks is that encryption (~90% of web traffic) obscures packet payloads, rendering traditional Deep Packet Inspection (DPI) ineffective for threat detection. AI/ML provides a solution by analyzing characteristics of encrypted traffic *without* decryption. Techniques include:
    - *Statistical Analysis:* Using features derived from packet lengths, sizes, inter-arrival times, and flow durations.
    - *Flow-Based Analysis:* Analyzing metadata and statistics of entire communication flows.
    - *TLS Handshake Analysis:* Extracting features from the unencrypted parts of the TLS handshake.
    - *Deep Learning:* Applying DL models (e.g., CNNs, RNNs) directly to raw packet data or sequence features to learn discriminative patterns indicative of specific applications or malicious activity. These methods enable classification of encrypted traffic types (e.g., browsing, streaming, malware C&C) and detection of anomalies hidden within encrypted flows.
- **Datasets and Evaluation:** The performance of AI/ML models heavily depends on the quality and representativeness of the training data. Realistic datasets capturing diverse 5G traffic patterns and attack scenarios are crucial but often difficult to obtain. Public datasets like CICIDS2017/2018 , CICDDoS2019 , AWID , and specialized 5G datasets like 5G-NIDD are used for research and evaluation. Performance is typically measured using metrics such as Accuracy, Precision, Recall, F1-Score, and ROC AUC.

AI/ML Technique	Detection Target	Key Strengths	Key Weaknesses/Challenges	Relevant Snippets
K-Nearest Neighbors (KNN)	General Intrusion, DDoS	Simple, Effective for some datasets, Good accuracy/ROC AUC reported	Computationally expensive for large datasets, Sensitive to feature scaling	
SVM	General Intrusion	Effective in high-dimensional spaces, Robust to overfitting	Computationally intensive training, Sensitive to kernel choice	
Decision Trees (DT)	General Intrusion, DDoS	Interpretable, Handles numerical/categorical data, Good recall reported	Prone to overfitting, Can be unstable	
Random Forest (RF)	General Intrusion, Signaling DDoS	High accuracy, Robust to overfitting, Handles high dimensions, Good performance reported	Less interpretable than single DTs, Can be slow on very large datasets	
Gradient Boosting (GB)	General Intrusion	Often achieves state-of-the-art performance, High accuracy reported	Sensitive to hyperparameters, Can overfit if not tuned carefully	
Naive Bayes (NB)	General Intrusion	Computationally efficient, Performs well with high dimensions	Assumes feature independence (often violated), Moderate accuracy reported	
Autoencoder (AE)	General Intrusion, HTTP/2 Anomalies	Unsupervised anomaly detection, Feature extraction/dimensionality reduction	Can be complex to train, Performance depends on architecture	
CNN	General Intrusion, Encrypted Traffic Analysis	Excellent for spatial hierarchies (e.g., image-like traffic representations), Feature learning	Requires large labeled datasets, Can be computationally expensive	
LSTM / BiLSTM	General Intrusion, Sequential Pattern Detection	Captures temporal dependencies in sequential data (e.g., packet sequences)	Complex to train, Can suffer from vanishing gradients	
GANs	Malicious Encrypted Traffic Generation/Detection	Can generate realistic data for training/augmentation, Adversarial learning	Training instability, Mode collapse	
Federated/Split Learning	Intrusion Detection (Privacy-Preserving)	Enables training on distributed data without centralizing raw data, Enhances privacy	Communication overhead, Potential model aggregation challenges, Security risks in aggregation	
Ensemble (e.g., Voting)	General Intrusion	Often improves robustness and accuracy over single models, Superior precision/F1 reported	Increased complexity	

Table 4 : Overview of AI/ML Techniques for 5G Anomaly Detection

Automated Threat Intelligence Analysis and Response

Beyond detection, AI/ML plays a crucial role in automating the analysis of threat intelligence and orchestrating security responses.

- AI for Threat Intelligence: AI/ML algorithms can ingest and analyze massive volumes of data from diverse sources – including network logs, endpoint data, SIEM alerts, external threat feeds, and vulnerability databases. By correlating events, identifying patterns, and understanding context, AI can :
    - Prioritize Alerts: Reduce "alert fatigue" by filtering out false positives and highlighting the most critical threats.
    - Identify Complex Attacks: Detect sophisticated, multi-stage attacks (Advanced Persistent Threats - APTs) that might evade simpler detection methods.
    - Predict Future Threats: Analyze historical data and current trends to forecast potential future attacks or vulnerabilities.

  - Contextualize Threats: Provide richer context around detected threats, aiding human analysts in investigation and response.
- Automated Response (SOAR): Security Orchestration, Automation, and Response (SOAR) platforms integrate various security tools (SIEM, firewalls, endpoint detection, threat intelligence platforms) into unified workflows. SOAR uses predefined "playbooks" to automate responses to specific types of security incidents. Automation can include actions like blocking malicious IP addresses at the firewall, isolating compromised endpoints, disabling user accounts, quarantining malicious files, or escalating complex incidents to human analysts. AI/ML significantly enhances SOAR capabilities by :
  - Intelligent Triage: AI analyzes incoming alerts to determine severity and select the appropriate playbook.
  - Adaptive Playbooks: ML allows playbooks to adapt based on the specific context of an incident or learn from past responses.
  - Automated Investigation: AI can automate parts of the investigation process, gathering relevant data and identifying root causes.
  - Faster Response: Automating the detection-to-response cycle drastically reduces reaction times, minimizing potential damage. Generative AI is also being integrated into SOAR for tasks like playbook creation and investigation assistance.
- **ETSI ENI (Experiential Networked Intelligence):** ETSI's ENI framework defines a cognitive network management architecture that utilizes AI/ML for closed-loop control based on the Observe-Orient-Decide-Act (OODA) model. While primarily focused on optimizing network operations, service assurance, and operator experience , ENI's principles of context-aware policy and automated decision-making could potentially be applied to security orchestration and response. ENI aims to enable networks to recognize changes and make actionable decisions, interacting with management systems to adjust services and resources. Its architecture involves AI analysis functional blocks processing normalized data. Recent work includes studies on AI agents for network slicing and intent policy management.
- **3GPP NWDAF (Network Data Analytics Function):** NWDAF is the standardized 5G Core function for network data analytics. It collects data from NFs, OAM, and UEs via standard interfaces (subscription or request-based) and provides analytics results (statistics or predictions) to authorized consumers (other NFs like PCF, AMF, SMF, NEF, or external systems). Standardized analytics types include load level prediction for slices/NFs, service experience prediction, UE mobility/behavior prediction, anomaly detection, and QoS sustainability prediction. NWDAF leverages ML models for these predictions. While primarily aimed at network optimization and automation , NWDAF's capabilities, particularly UE abnormal behavior detection and load/congestion analytics, can provide valuable input for security monitoring and potentially trigger automated security responses via interaction with other NFs (e.g., PCF for policy changes). NWDAF can be deployed centrally or distributed (e.g., at the edge) to meet varying latency requirements.

A dynamic exists between relying on standardized frameworks like NWDAF and ENI, which ensure interoperability but may offer baseline capabilities, and adopting more advanced, potentially proprietary AI/ML solutions from vendors. Standards define interfaces and common analytics types, simplifying data collection and consumption. However, cutting-edge threat detection and response often rely on sophisticated, vendor-specific algorithms and models trained on extensive datasets. This presents operators with a choice between prioritizing interoperability through standards or potentially achieving higher security efficacy with proprietary tools, risking vendor lock-in. A hybrid approach, using standardized interfaces like NWDAF for data acquisition while integrating specialized AI/ML security engines for analysis and response, appears likely. Open architectures like O-RAN might further facilitate the integration of diverse AI tools.

Furthermore, the effectiveness of any AI/ML security system hinges critically on the availability and quality of data. Obtaining large-scale, realistic, and accurately labeled 5G network traffic datasets, especially those containing diverse and modern attack vectors, remains a significant challenge due to practical difficulties and privacy constraints. Encryption further complicates data analysis, forcing reliance on metadata and statistical features. Privacy regulations limit the use of sensitive subscriber data, potentially hindering user behavior analytics. The dynamic nature of 5G also requires continuous data collection and model retraining to prevent performance degradation. Addressing these data challenges through better dataset creation, privacy-enhancing technologies (like federated learning), and robust model design is crucial for realizing the full potential of AI/ML in 5G security.

VI. The Synergy of ZTA and AI/ML for Adaptive 5G Security

Neither ZTA nor AI/ML alone can fully address the security complexities of 5G. However, their integration creates a powerful synergy, leading to a more robust, adaptive, and intelligent security framework.

Towards a Robust and Adaptive Security Framework

ZTA and AI/ML play complementary roles in securing 5G networks. ZTA provides the foundational security philosophy and architectural principles: eliminate implicit trust, enforce least privilege access, implement micro-segmentation, and continuously verify. It defines the desired security posture and the rules of engagement. However, implementing and managing these principles dynamically at the scale and speed of 5G is challenging. This is where AI/ML provides the necessary intelligence and automation.

AI/ML enhances ZTA implementation in several key ways:

- **Intelligent and Dynamic Policy Enforcement:** AI/ML algorithms can analyze a wide range of real-time contextual information – user behavior patterns, device security posture (from CDM systems), threat intelligence feeds, network conditions (potentially sourced via NWDAF), application behavior – to make more nuanced and accurate risk assessments. This allows the ZTA Policy Engine (PE) to move beyond static rules and implement truly dynamic, risk-adaptive access policies. Access can be granted, denied, or adjusted based on the real-time calculated trust score of the requesting subject and target resource.
- **Enhanced Continuous Monitoring:** AI/ML powers the continuous monitoring and validation tenet of ZTA. By learning normal behavior baselines for users, devices, NFs, and applications, AI/ML can detect subtle anomalies, zero-day threats, or insider threats that might otherwise go unnoticed by rule-based systems. This provides critical input for ZTA trust assessments and policy decisions.
- **Automated Response Orchestration:** When AI/ML systems detect a high-risk event or a policy violation, they can automatically trigger enforcement actions through the ZTA framework (via the PA/PEP) or integrated SOAR platforms. This could involve revoking access credentials, quarantining a device, isolating a network micro-segment, or initiating specific remediation workflows, enabling much faster response times than manual intervention allows.

Conversely, ZTA provides a structured environment that benefits AI/ML deployment:

- **Clear Security Objectives:** ZTA principles (LPA, verify everything) provide clear goals for AI/ML algorithms to optimize towards.
- **Rich Contextual Data:** The continuous monitoring and verification inherent in ZTA generate rich streams of data (access logs, device posture, traffic flows within segments) that can be used to train and refine AI/ML models.
- **Containment for AI Risks:** Micro-segmentation, a core ZTA concept, can help contain the potential impact if an AI model itself is compromised or behaves unexpectedly.
- **Defined Enforcement Points:** ZTA's PEPs provide clear points in the architecture where AI-driven decisions can be enforced.

This synergy leads to an adaptive security framework where ZTA defines the rules and structure, and AI/ML provides the dynamic intelligence and automation to enforce those rules effectively at scale, continuously learning and adapting to the evolving threat landscape. Concepts like the "intelligent ZTA" (i-ZTA) explicitly envision this deep integration , and commercial solutions are emerging that combine AI-powered threat detection with ZTA principles for 5G. The application of AI-driven ZTA is particularly relevant for securing open architectures like O-RAN.

Balancing Security Efficacy and Privacy Considerations

The powerful capabilities of ZTA and AI/ML also introduce potential privacy concerns. ZTA relies on continuous monitoring and detailed logging of access requests and user/device behavior. AI/ML often requires access to vast amounts of data, potentially including sensitive user information or communication patterns, for effective training and analysis. This creates a tension between achieving granular security control and protecting user privacy.

Addressing this requires careful consideration and implementation of privacy-preserving measures:

- **Data Minimization and Governance:** Implementing strict data governance policies that define precisely what data is collected, its purpose (specifically for security analysis and ZTA enforcement), how long it's retained, and who can access it. The principle of collecting only necessary data should be applied.
- **Privacy-Enhancing Technologies (PETs):** Exploring and potentially deploying PETs can help mitigate privacy risks. Techniques like data anonymization or pseudonymization can obscure identities in datasets. Differential privacy can add noise to query results or model outputs to prevent inference about individuals. Federated learning allows ML models to be trained on distributed data (e.g., at the edge or on user devices) without centralizing the raw data, although it introduces its own complexities and potential security risks.
- **Transparency and Explainability:** Ensuring transparency in how ZTA policies are enforced and how AI/ML models arrive at their decisions (Explainable AI - XAI) is crucial for building user trust, enabling audits, and identifying potential biases or errors.
- **Secure Data Handling:** Protecting the collected monitoring data and the AI models themselves from unauthorized access or tampering is essential. ZTA principles should also be applied to the security analytics infrastructure itself.

Achieving a balance requires integrating privacy considerations into the design of the ZTA and AI/ML security framework from the outset, rather than treating privacy as an afterthought.

Role of Industry Standards and Future Outlook

Standardization plays a critical role in establishing baseline security and interoperability for 5G, ZTA, and AI/ML integration, although gaps remain.

- **Standards Landscape:** Several Standards Development Organizations (SDOs) and industry bodies contribute to the 5G security ecosystem:
    - *3GPP:* Defines the core 5G architecture and fundamental security features (authentication, encryption, privacy, SBA security, SEPP, NWDAF) in specifications like TS 33.501, TS 23.501/502, TS 29.520.
    - *ETSI:* Develops standards for enabling technologies like NFV (including security aspects), MEC (including security), and cognitive network management via AI/ML (ENI).
    - *NIST:* Provides foundational guidance on cybersecurity frameworks, including the widely referenced ZTA model in SP 800-207.
    - *O-RAN Alliance:* Focuses on defining open interfaces and architectures for the RAN, incorporating security requirements and ZTA principles.
    - *GSMA:* Publishes security guidelines, particularly for interconnect and roaming security (e.g., FS.19 for Diameter, FS.21 for signaling, FS.36 for 5G interconnect).
    - *ENISA:* The EU Agency for Cybersecurity provides threat landscape analysis and security recommendations for 5G.
- **Gaps and Evolution:** While these standards provide essential building blocks, they do not yet offer a complete, standardized blueprint for a fully AI-driven ZTA in the 5G telecom context. Gaps exist in areas like standardized interfaces for advanced AI/ML integration beyond basic NWDAF analytics, end-to-end ZTA orchestration across multi-vendor domains, and security assurance for complex AI models. Security is a continuous process, with standards evolving through ongoing releases (e.g., 3GPP Release 18 and beyond focusing on areas like enhanced slice security, AI/ML integration, and potentially post-quantum security). The evolution towards 5G-Advanced and 6G will likely see deeper integration of AI/ML, necessitating further standardization efforts.
- **Convergence of IT and Telecom Security:** The adoption of IT-derived technologies (cloud, virtualization, APIs, SDN) and security paradigms (ZTA, AI/ML analytics, SOAR) in 5G signifies a crucial convergence between the traditionally distinct worlds of telecom and IT security. 5G's architecture necessitates leveraging security principles and tools honed in the enterprise IT space (like ZTA) to address vulnerabilities arising from its software-based, distributed nature. Simultaneously, the scale, real-time performance demands, and reliability requirements of telecom networks necessitate adapting and optimizing these IT security approaches for the 5G context. This convergence requires cross-domain expertise and closer collaboration between telecom operators, equipment vendors, cloud providers, and cybersecurity specialists, as well as coordination between relevant standards bodies.
- **Future Research Directions:** Continued research is vital to address remaining challenges and enhance future network security. Key areas include:
    - Developing highly accurate, efficient, and explainable AI/ML models for detecting sophisticated

threats, especially within encrypted traffic.

- Designing scalable, low-latency ZTA enforcement mechanisms suitable for URLLC and massive-scale deployments.
- Creating provably secure isolation techniques for network slicing and virtualized functions.
- Securing AI/ML models themselves against adversarial attacks (e.g., data poisoning, evasion, model stealing).
- Integrating post-quantum cryptography (PQC) into 5G and future network standards to address threats from quantum computing.
- Developing standardized frameworks and metrics for quantifying trust and security posture in dynamic, multi-domain 5G environments.
- Refining privacy-enhancing technologies for use in security monitoring and AI training.

Standardization Body	Key Specification/Document Area	Relevant Specification/Document IDs (Examples)	Brief Description of Scope/Contribution
3GPP	Overall 5G System Architecture	TS 23.501 , TS 23.502 , TS 23.503	Defines overall 5G architecture (RAN, Core, SBA), NFs, procedures, including basic security principles.
	Security Architecture & Procedures	TS 33.501	Primary specification for 5G security architecture, authentication (5G-AKA), key hierarchy, privacy (SUCI), SBA security, SEPP, NAS/AS security.
	Network Slicing Security	TR 33.813 , TS 33.501 updates	Specifies security aspects for network slicing, including NSSAA, NF authorization per slice, S-NSSAI protection.
	Network Data Analytics Function (NWDAF)	TS 23.288, TS 29.520	Defines the NWDAF for collecting data and providing network analytics, including standard interfaces and analytics types (some relevant to security).
	Security Assurance Specifications (SCAS)	TS 33.xxx series (e.g., for NFs)	Defines security requirements and test cases for specific 5G network functions/products.
ETSI	Network Functions Virtualization (NFV) Security	Various ETSI GS NFV-SEC documents	Addresses security aspects of the NFV framework, including MANO, NFVI, and VNFs.
	Multi-Access Edge Computing (MEC) Security	Various ETSI GS MEC documents (e.g., MEC 009 APIs, GR MEC 031 5G integration)	Defines MEC architecture, APIs, and addresses security challenges specific to edge deployments (platform, application, federation security).
	Experiential Networked Intelligence (ENI)	Various ETSI GS/GR ENI documents (e.g., GS ENI 005 Architecture)	Defines architecture for AI/ML-based cognitive network management, potentially applicable to automated security operations.
	Cybersecurity (TC CYBER)	Various ETSI TS/TR documents	Develops broader cybersecurity standards potentially applicable to 5G and related technologies (e.g., IoT security, cryptography).
NIST	Zero Trust Architecture (ZTA)	SP 800-207	Provides foundational concepts, tenets, logical components, and deployment models for ZTA (technology agnostic).

	Risk Management Framework (RMF)	SP 800-37	Framework for managing organizational risk, relevant context for ZTA implementation.
O-RAN Alliance	Open RAN Security	O-RAN Security Threat Modeling, Security Requirements Specifications, etc.	Defines security requirements and architectures specifically for the open, multi-vendor O-RAN environment, explicitly adopting ZTA principles.
GSMA	Interconnect & Roaming Security	FS.19 (Diameter), FS.21 (Signaling), FS.36 (5G Interconnect), FS.11 (GTP)	Provides guidelines and recommendations for operators to secure signaling and data interconnects between networks, addressing protocol vulnerabilities.
ENISA	5G Threat Landscape & Security Analysis	ENISA Threat Landscape for 5G Networks report	Provides comprehensive analysis of 5G threats, vulnerabilities, and security considerations based on architecture and use cases.

Table 5 : Key 5G Security Standards and Specifications Landscape

VII. Conclusion

The fifth generation of mobile networks heralds an era of unprecedented connectivity and technological capability, fundamentally reshaping industries and daily life. However, the architectural underpinnings of 5G—virtualization, software-defined networking, service-based architecture, network slicing, and edge computing—while enabling this transformation, concurrently introduce a significantly expanded and more complex security and privacy landscape compared to previous generations. Traditional perimeter-based security models are demonstrably insufficient to protect against the diverse array of threats targeting 5G systems, including sophisticated signaling attacks, large-scale DDoS campaigns amplified by IoT, advanced spoofing techniques, and vulnerabilities inherent in shared and distributed resources.

This analysis has detailed the core security challenges posed by 5G and critically evaluated the potential of Zero Trust Architecture (ZTA) and Artificial Intelligence/Machine Learning (AI/ML) as essential components of a modern defense strategy. ZTA provides a crucial philosophical shift towards "never trust, always verify," mandating continuous authentication, authorization, least privilege access, and micro-segmentation across the entire ecosystem (UE, RAN, Core, Edge, Slices, Management). While 3GPP and other standards bodies provide foundational security features that support ZTA, its full implementation requires a holistic approach integrating these features with dynamic policy enforcement and continuous monitoring.

However, the scale, speed, and complexity of 5G make manual implementation and static enforcement of ZTA principles impractical. AI/ML emerges as the critical enabler, providing the necessary intelligence and automation. AI/ML algorithms offer advanced capabilities for real-time anomaly detection (even in encrypted traffic), predictive threat intelligence analysis, and automated security response orchestration (e.g., via SOAR platforms or integrated functions like NWDAF/ENI).

The true strength lies in the synergy between ZTA and AI/ML. ZTA establishes the robust security framework and principles, while AI/ML provides the dynamic, adaptive intelligence required to enforce these principles effectively and efficiently at 5G scale. This combination allows for a security posture that can continuously learn and adapt to the evolving threat landscape. Nonetheless, challenges related to implementation complexity, performance impact, interoperability, scalability, and balancing security with user privacy must be carefully addressed.

Ensuring the security and trustworthiness of 5G and future networks is not solely a technical challenge but requires ongoing collaboration between network operators, technology vendors, researchers, standardization bodies, and policymakers. Continued efforts in refining standards, developing robust and privacy-preserving AI/ML techniques, addressing emerging threats (such as those related to AI security itself and quantum computing), and fostering a security-conscious ecosystem are paramount. By embracing adaptive security frameworks built upon the synergistic integration of ZTA and AI/ML, the full potential of 5G can be realized securely and reliably.

REFERENCES

1. 3GPP 5G Core Network: An Overview and Future Directions - Journal of Information and Communication Convergence Engineering, https://www.jicce.org/journal/view.html?pn=myread&uid=2&vmd=Full
2. 5G System Overview - 3GPP, https://www.3gpp.org/technologies/5g-system-overview
3. Service-Based Architecture in 5G - Insert Title in Document properties, https://www.ngmn.org/wp-content/uploads/Publications/2018/180119_NGMN_Service_Based_Architecture_in_5G_v1.0.pdf
4. 5G Security Threat Assessment in Real Networks - PMC - PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC8399903/
5. (PDF) Integration of Edge Computing in 5G RAN: Deploying Low-Latency and High-Efficiency Networks - ResearchGate, https://www.researchgate.net/publication/389689193_Integration_of_Edge_Computing_in_5G_RAN_Deploying_Low-Latency_and_High-Efficiency_Networks
6. Hidden 5G Challenges: What Telecom Providers Must Know About IoT Integration, https://wds-sicap.com/news-events/hidden-5g-challenges
7. 5G vs 4G:Speed, Latency, and Advancements in 5G Networks - Cavli Wireless, https://www.cavliwireless.com/blog/nerdiest-of-things/5g-vs-4g-differences-advantages-speed-latency-network-slicing
8. Choosing Between 4G LTE and 5G: What Network Evolution Means for Industrial Connectivity - Taoglas, https://www.taoglas.com/blogs/choosing-between-4g-lte-and-5g-what-network-evolution-means-for-industrial-connectivity/
9. Exploring the technological advancements and security issues of 5G, https://wjarr.com/sites/default/files/WJARR-2024-2367.pdf
10. Investigation and Technological Comparison of 4G and 5G Networks, https://www.scirp.org/journal/paperinformation?paperid=106688
11. Understanding 5G Security: Key Challenges and Solutions - Wray Castle, https://wraycastle.com/blogs/knowledge-base/understanding-5g-security-key-challenges-and-solutions
12. A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas - DigitalCommons@UNL, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1751&context=electricalengineeringfacpub
13. Exploring Emerging Trends in 5G Malicious Traffic Analysis and Incremental Learning Intrusion Detection Strategies - arXiv, https://arxiv.org/html/2402.14353v1
14. From Telit: 5G IoT Security Issues: A Guide to Next-Gen Wireless ..., https://www.symmetryelectronics.com/blog/5g-iot-security-issues-a-guide-to-next-gen-wireless-network-risks/
15. PRIVACY & DATA SECURITY IN 5G NETWORKS - ABI Research, https://go.abiresearch.com/hubfs/Marketing/Whitepapers/Privacy%20and%20Data%20Security%20in%205G%20Networks/ABI_Research_Privacy_and_Data_Security_in_5G_Networks.pdf
16. (PDF) A Comparison of 4G LTE and 5G Network Cybersecurity Performance, https://www.researchgate.net/publication/381044175_A_Comparison_of_4G_LTE_and_5G_Network_Cybersecurity_Performance
17. From 4G to 5G: Security Concerns and Public Wi-Fi | DNSFilter, https://www.dnsfilter.com/blog/compare-5g-4g-public-wi-fi-security
18. Real-time DDoS Defense in 5G-Enabled IoT: A Multidomain Collaboration Perspective, https://www.researchgate.net/publication/365104781_Real-time_DDoS_Defense_in_5G-Enabled_IoT_A_Multidomain_Collaboration_Perspective
19. (PDF) Securing 5G virtual networks: a critical analysis of SDN, NFV ..., https://www.researchgate.net/publication/383265822_Securing_5G_virtual_networks_a_critical_analysis_of_SDN_NFV_and_network_slicing_security
20. ENISA Report – Threat Landscape for 5G Networks - IAPP, https://iapp.org/resources/article/enisa-report-threat-landscape-for-5g-networks/
21. A Deep Dive into 5G Service-Based Architecture (SBA) - Calsoft Blog, https://www.calsoftinc.com/blogs/5g-service-based-architecture-sba.html
22. Integration of Edge Computing in 5G RAN: Deploying Low-Latency and High-Efficiency Networks - IJIRMPS, https://www.ijirmps.org/papers/2019/5/231869.pdf
23. 3.3 3GPP 5G Architecture | Overview of 5G Use Cases and Architecture - InformIT, https://www.informit.com/articles/article.aspx?p=3128834&seqNum=3
24. An Integrated Software-Defined Networking–Network Function Virtualization Architecture for 5G RAN–Multi-Access Edge Computing Slice Management in the Internet of Industrial Things - MDPI, https://www.mdpi.com/2073-431X/13/9/226
25. What is the 5G Service-Based Architecture (SBA)? | Microsoft ..., https://techcommunity.microsoft.com/blog/telecommunications-industry-blog/what-is-the-5g-service-based-architecture-sba/3831367

26. 5G CORE NETWORK - Telecommunication Engineering Centre, https://www.tec.gov.in/public/pdf/Studypaper/5G%20Core%20Network_Study%20Paper_v8.pdf 27. Automated Attack and Defense Framework for 5G Security on Physical and Logical Layers - arXiv, https://arxiv.org/pdf/1902.04009
28. Understanding NIST 800-207 - RiskRecon, https://blog.riskrecon.com/understanding-nist-800-207
29. Zero Trust Architecture: The Ultimate Guide to Modern Network Security - BuzzClan, https://buzzclan.com/cyber-security/zero-trust-architecture/
30. www.cyberark.com, https://www.cyberark.com/what-is/nist-sp-800-207-cybersecurity-framework/#:~:text=NIST%20SP%20800%2D207%20introduces,the%20network%2C%20is%20automatically%20trusted.
31. What is Zero Trust? - Guide to Zero Trust Security - CrowdStrike, https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/
32. What is Zero Trust Architecture? - Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
33. 5G Security Threat Landscape, AI and Blockchain - ResearchGate, https://www.researchgate.net/publication/378142250_5G_Security_Threat_Landscape_AI_and_Blockchain
34. A Complete EDA and DL Pipeline for Softwarized 5G Network Intrusion Detection - MDPI, https://www.mdpi.com/1999-5903/16/9/331
35. 5G Americas Examines Trust and Security in AI-Powered Wireless Networks, https://www.5gamericas.org/5g-americas-examines-trust-and-security-in-ai-powered-wireless-networks/
36. A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond - MDPI, https://www.mdpi.com/2227-7390/13/7/1088
37. AI-powered network optimization: Unlocking 5G's potential with Amdocs - Google Cloud, https://cloud.google.com/blog/topics/telecommunications/ai-powered-network-optimization-unlocking-5gs-potential-with-amdocs
38. AI in 5G Network Security: Revolutionizing Threat Detection - Mischa Dohler, https://mischadohler.com/ai-in-5g-network-security-revolutionizing-threat-detection/
39. What Is the Role of AI in Security Automation? - Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-in-security-automation
40. A 5G-Edge Architecture for Computational Offloading of Computer Vision Applications, https://arxiv.org/html/2501.04267v1
41. ETSI Mobile Security Standards May 2022 - EU Cyber Acts Conference, https://eucyberact.org/wp-content/uploads/2022/05/P10a-LeadbeaterA.pdf
42. 5G Radio Access Network Architecture: The Dark Side of 5G (IEEE Press) - Amazon.com, https://www.amazon.com/5G-Radio-Access-Network-Architecture/dp/1119550882
43. Toward Zero Trust Security IN 5G Open Architecture Network Slices - ResearchGate, https://www.researchgate.net/publication/367398508_Toward_Zero_Trust_Security_IN_5G_Open_Architecture_Network_Slices
44. Enhancing mobile network security: Why Open RAN needs ZTA and DPI - ipoque GmbH, https://www.ipoque.com/blog/zero-trust-and-dpi-in-open-ran
45. O-RAN ALLIANCE Sets AI-Driven RAN Priorities for Global 5G & 6G Deployment, https://www.thefastmode.com/technology-solutions/40662-o-ran-alliance-sets-ai-driven-ran-priorities-for-global-5g-6g-deployment
46. 5G Core Network (5GC) Functions - Grandmetric Blog, https://www.grandmetric.com/5g-core-network-functions/
47. The 5G System Architecture - SciSpace, https://scispace.com/pdf/the-5g-system-architecture-nnfbs8e2rp.pdf
48. 5G Service-Based Architecture - Devopedia, https://devopedia.org/5g-service-based-architecture
49. 5GShield: HTTP/2 Anomaly Detection in 5G Service-Based Architecture - ResearchGate, https://www.researchgate.net/publication/372616042_5GShield_HTTP2_Anomaly_Detection_in_5G_Service-Based_Architecture
50. 5G-WAVE: A Core Network Framework with Decentralized Authorization for Network Slices - arXiv, https://arxiv.org/pdf/2404.13242
51. Advancing DDoS Detection in 5G Networks Through Machine Learning and Deep Learning Techniques - DiVA portal, http://www.diva-portal.org/smash/get/diva2:1876552/FULLTEXT01.pdf
52. 5G Security Solution Overview - F5, https://www.f5.com/pdf/solution-overview/establishing-5g-security.pdf
53. Architectural and Cost Implications of the 5G Edge NFV Systems, https://par.nsf.gov/servlets/purl/10174802
54. How does mobile edge computing work? - 5G Technology World, https://www.5gtechnologyworld.com/how-does-mobile-edge-computing-work/ 55. 5G Multi-access Edge Computing: a Survey on Security, Dependability, and Performance - arXiv, https://arxiv.org/pdf/2107.13374
56. Edge vs. Core - An Increasingly Less Pronounced Distinction in 5G Networks - CISA, https://www.cisa.gov/sites/default/files/publications/5g_edge-core-computing_508.pdf
57. White Paper on MEC security; Status of standards support and future evolutions - ETSI, https://www.etsi.org/images/files/etsiwhitepapers/etsi-wp-46-2nd-ed-mec-security.pdf
58. MEC security: Status of standards support and future evolutions - ETSI, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_WP_46-_MEC_security.pdf
59. ETSI publishes white paper on Edge computing security - IOT Insider, https://www.iotinsider.com/news/etsi-publishes-white-paper-on-edge-computing-security/
60. ETSI webinar - BrightTALK, https://www.brighttalk.com/resource/core/418238/2022_12_12---etsi-webinar-on-mec-security---v10_892569.pdf
61. 5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection - arXiv, https://arxiv.org/pdf/2304.05719
62. Leveraging SDN for The 5G Networks: Trends, Prospects and Challenges - arXiv, https://arxiv.org/pdf/1506.02876

63. (PDF) Network Slicing Security: Challenges and Directions - ResearchGate, https://www.researchgate.net/publication/334754494_Network_Slicing_Security_Challenges_and_Directions
64. CYBERSECURITY IN 5G: A REVIEW OF VULNERABILITIES AND THREAT PREVENTION STRATEGIES - The Roman Science Publications and Distributions, https://romanpub.com/resources/Vol%204%20%2C%20No%203%20-%2031.pdf
65. (PDF) Security in 5G Network Slices: Concerns and Opportunities - ResearchGate, https://www.researchgate.net/publication/379715494_Security_in_5G_Network_Slices_Concerns_and_Opportunities
66. Network Slicing Security for 5G and 5G Advanced Systems - 3GPP, https://www.3gpp.org/technologies/slicing-security
67. Realizing a zero-trust architecture for 5G networks | Nokia.com, https://www.nokia.com/bell-labs/bell-labs-consulting/articles/realizing-zero-trust-architecture-for-5g-networks/
68. Zero-Trust Data Security in 5G Networks - Dell Technologies Info Hub, https://infohub.delltechnologies.com/t/zero-trust-data-security-in-5g-networks/
69. Multi-Stage Threat Modelling and Security Monitoring in 5GCN - arXiv, https://arxiv.org/pdf/2108.11207
70. Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey - MDPI, https://www.mdpi.com/2079-9292/13/10/1860
71. Addressing Cybersecurity Threats in 5G Network Slicing | We Are CORTEX, https://www.wearecortex.com/blog/how-can-you-deal-with-cybersecurity-threats-to-network-slicing-and-the-usrp/
72. [1809.06925] Security and Protocol Exploit Analysis of the 5G Specifications - ar5iv - arXiv, https://ar5iv.labs.arxiv.org/html/1809.06925
73. 5G SUCI-catchers: still catching them all? | Request PDF - ResearchGate, https://www.researchgate.net/publication/352796449_5G_SUCI-catchers_still_catching_them_all
74. A Survey on 5G Wireless Network Intrusion Detection Systems Using Machine Learning Techniques | Request PDF - ResearchGate, https://www.researchgate.net/publication/388110388_A_Survey_on_5G_Wireless_Network_Intrusion_Detection_Systems_Using_Machine_Learning_Techniques
75. Obtain subscriber identifier via NF - MITRE | FiGHT™, https://fight.mitre.org/techniques/FGT5019.003/
76. An overview of the 3GPP 5G security standard - Ericsson, https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview 77. Security for 5G - ShareTechnote, https://www.sharetechnote.com/html/5G/5G_Security.html
78. Delving into SUPI, SUCI, and 5G-GUTI in 5G SA Networks - 5GWorldPro.com, https://www.5gworldpro.com/blog/2025/02/28/delving-into-supi-suci-and-5g-guti-in-5g-sa-networks/
79. Roaming Security in 5G Systems⋆ - NTNU, https://www.ntnu.no/ojs/index.php/nikt/article/download/5651/5258/21735
80. draft_S3-190948-v2 Enhanced Network slicing TR 33813-030-rm.docx - 3GPP, https://www.3gpp.org/ftp/Inbox/SA3/Inbox/drafts/draft_S3-190948-v2%20Enhanced%20Network%20slicing%20TR%2033813-030-rm.docx
81. Interworking Security - GSMA, https://www.gsma.com/solutions-and-impact/technologies/security/cybersecurity-knowledge-base/interworking-security/
82. SVI-IWF Diameter Interworking Function - Squire Technologies, https://squire-technologies.co.uk/products/diameter-interworking-function/
83. Overview of 5G Security and Vulnerabilities - The Cyber Defense Review, https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf
84. A Comprehensive Review of 5G System Security, https://ijarsct.co.in/Paper17427.pdf
85. [2108.08700] 5G System Security Analysis - ar5iv, https://ar5iv.labs.arxiv.org/html/2108.08700
86. The Top 4 DDoS Attack Vectors Threatening 5G Networks - Allot, https://www.allot.com/blog/top-ddos-attack-vectors-threatening-5g/
87. Machine Learning Based Signaling DDoS Detection System for 5G Stand Alone Core Network - OUCI, https://ouci.dntb.gov.ua/en/works/leRNKGK9/
88. Machine Learning Based Signaling DDoS Detection System for 5G Stand Alone Core Network - MDPI, https://www.mdpi.com/2076-3417/12/23/12456
89. (PDF) A TELCO ODYSSEY: 5G SUCI-CRACKER AND SCTP-HIJACKER - ResearchGate, https://www.researchgate.net/publication/365375770_A_TELCO_ODYSSEY_5G_SUCI-CRACKER_AND_SCTP-HIJACKER
90. Bridging the Security Gap: Lessons from 5G and What 6G Should Do Better - arXiv, https://arxiv.org/html/2501.11045v1
91. Survey on 5G Physical Layer Security Threats and Countermeasures - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC11397919/
92. GNSS Spoofing Detection and Mitigation With a Single 5G Base Station Aiding, https://www.researchgate.net/publication/379377949_GNSS_Spoofing_Detection_and_Mitigation_With_a_Single_5G_Base_Station_Aiding
93. GPS Spoofing Detector with Adaptive Trustable Residence Area for Cellular based-UAVs - MOSAIC Lab, http://www.mosaic-lab.org/uploads/papers/da7d181b-be4b-446d-bd8f-0dadfb754c39.pdf
94. 5G Hardware Supply Chain Security Through Physical Measurements - NIST Technical Series Publications, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1278.pdf
95. What is the NIST SP 800-207 cybersecurity framework? - CyberArk, https://www.cyberark.com/what-is/nist-sp-800-207-cybersecurity-framework/
96. Defining Zero Trust:, https://api.ctia.org/wp-content/uploads/2023/01/Defining-Zero-Trust-White-Paper-2023.pdf
97. Enabling a Zero Trust Architecture in a 5G-enabled Smart Grid - arXiv, https://arxiv.org/pdf/2210.01739
98. NIST 800-207: Zero Trust Architecture | NextLabs, https://www.nextlabs.com/wp-content/uploads/2024/11/NextLabs-White-Paper-NIST-800-207-Zero-Trust-Architecture.pdf

99. Zero Trust Architecture - NIST Technical Series Publications, https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
100. Adopting zero trust for private 5G - Capgemini Norway, https://www.capgemini.com/no-no/insights/expert-perspectives/adopting-zero-trust-for-private-5g/
101. Zero Trust Security & Private 5G: The Future of Cyber Defense - NYBSYS, https://nybsys.com/zero-trust-security/
102. Zero Trust Architecture (ZTA) Explained - NIST 800-207, https://getnametag.com/newsroom/nist-800-207-zero-trust-architecture-zta-explained
103. nvlpubs.nist.gov, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
104. Zero Trust Architecture for advancing mobile network security operations - Ericsson, https://www.ericsson.com/en/reports-and-papers/white-papers/network-resilience-through-zero-trust-architecture
105. Implement Zero Trust as Defined by NIST 800-207 - iboss, https://www.iboss.com/storage/2022/02/2022_iboss-implement-zero-trust-ebook.pdf?vgo_ee=XccgWu2nR7KN%2BDKn9sA9ePa0%2F5Hgz2O1pL9JAq1RE8Q%3D
106. Embracing Zero Trust Security for Enhanced 5G Network Protection - Comviva, https://www.comviva.com/blog/embracing-zero-trust-security-for-enhanced-5g-network-protection/
107. 5G zero trust – A Zero-Trust Architecture for Telecom - ResearchGate, https://www.researchgate.net/publication/365433024_5G_zero_trust_-_A_Zero-Trust_Architecture_for_Telecom
108. Zero trust security framework: benefits and downsides - Verizon, https://www.verizon.com/business/resources/articles/s/zero-trust-security-framework-benefits-and-downsides/
109. Addressing complexities of zero trust implementation in OT/ICS environments to bolster cybersecurity - Industrial Cyber, https://industrialcyber.co/features/addressing-complexities-of-zero-trust-implementation-in-ot-ics-environments-to-bolster-cybersecurity/
110. (PDF) Enhancing Enterprise Security with Zero Trust Architecture - ResearchGate, https://www.researchgate.net/publication/385215775_Enhancing_Enterprise_Security_with_Zero_Trust_Architecture
111. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model, https://pmc.ncbi.nlm.nih.gov/articles/PMC10892953/
112. 5G zero trust – a zero-trust architecture for telecom - Ericsson, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g
113. (PDF) Toward Zero Trust Security IN 5G OPEN ARCHITECTURE NETWORK SLICES, https://www.researchgate.net/publication/377334836_Toward_Zero_Trust_Security_IN_5G_OPEN_ARCHITECTURE_NETWORK_SLICES
114. A Case for Enabling Delegation of 5G Core Decisions to the RAN - arXiv, https://arxiv.org/html/2408.07853v1
115. (PDF) Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning - ResearchGate, https://www.researchgate.net/publication/351342318_Intelligent_Zero_Trust_Architecture_for_5G6G_Tactical_Networks_Principles_Challenges_and_the_Role_of_Machine_Learning
116. TS 133 501 - V15.2.0 - 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.2.0 Release 15) - ETSI, https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf
117. Zero Trust Architecture enabled by 3GPP security - Ericsson, https://www.ericsson.com/en/blog/2025/2/zero-trust-architecture-enabled-by-3gpp-security
118. zero trust architectures: are we there yet? | mitre, https://www.mitre.org/sites/default/files/2021-12/pr-21-1273-zero-trust-architectures-are-we-there-yet.pdf
119. Intelligent zero trust architecture for 5G/6G networks - ANDRO Computational Solutions, https://www.androcs.com/wp/wp-content/uploads/2023/08/RamezanpourZTA22.pdf
120. Benefits & Challenges of Zero Trust: What Businesses Need to Know - NordLayer, https://nordlayer.com/learn/zero-trust/benefits/
121. Securing the 5G Core: Challenges and Solutions - Palo Alto Networks, https://www.paloaltonetworks.com/cybersecurity-perspectives/securing-the-5g-core-challenges-and-solutions
122. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC9782871/
123. Anomaly detection in encrypted HTTPS traffic using machine learning: a comparative analysis of feature selection techniques, https://mesopotamian.press/journals/index.php/cs/article/download/66/81/1560
124. Intrusion Detection in 5G and Wi-Fi networks: A Survey of Current Methods, Challenges & Perspectives - ResearchGate, https://www.researchgate.net/publication/389413824_Intrusion_Detection_in_5G_and_Wi-Fi_networks_A_Survey_of_Current_Methods_Challenges_Perspectives
125. Applications of Machine Learning in Cyber Security: A Review - MDPI, https://www.mdpi.com/2624-800X/4/4/45
126. What Is the Role of AI and ML in Modern SIEM Solutions? - Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-and-machine-learning-ml-in-siem
127. Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond - MDPI, https://www.mdpi.com/1424-8220/22/24/9957
128. Wireless Intrusion and Attack Detection for 5G Networks using Deep Learning Techniques, https://thesai.org/Publications/ViewPaper?Volume=12&Issue=7&Code=IJACSA&SerialNo=95
129. Enhancing Security in 5G Edge Networks: Predicting Real-Time Zero Trust Attacks Using Machine Learning in SDN Environments - MDPI, https://www.mdpi.com/1424-8220/25/6/1905

130. Enhance Private 5G Security for Industrial Deployments - Palo Alto Networks, https://www.paloaltonetworks.com/blog/2025/03/enhance-private-5g-security/
131. Machine Learning-Powered Encrypted Network Traffic Analysis: A Comprehensive Survey | Request PDF - ResearchGate, https://www.researchgate.net/publication/363718774_Machine_Learning-Powered_Encrypted_Network_Traffic_Analysis_A_Comprehensive_Survey
132. AI-Based Malicious Encrypted Traffic Detection in 5G Data Collection and Secure Sharing, https://www.mdpi.com/2079-9292/14/1/51
133. SOAR: Security Orchestration, Automation and Response in Cybersecurity - Calsoft Blog, https://www.calsoftinc.com/blogs/soar-security-orchestration-automation-and-response-in-cybersecurity.html
134. Google Security Operations - Response, https://cloud.google.com/security/products/security-orchestration-automation-response
135. 5G Security for Service Providers - Palo Alto Networks, https://www.paloaltonetworks.com/network-security/5g-for-service-providers
136. AI/ML in Security Orchestration, Automation and Response: Future Research Directions, https://www.researchgate.net/publication/350549572_AIML_in_Security_Orchestration_Automation_and_Response_Future_Research_Directions
137. Experiential Networked Intelligence (ENI) - ETSI, https://www.etsi.org/technologies/experiential-networked-intelligence
138. Our group Experiential Networked Intelligence (ENI) - ETSI, https://www.etsi.org/committee/1423-eni
139. ETSI Experiential Networked Intelligence – Release 2 Explained, https://techblog.comsoc.org/2022/01/15/etsi-release-2-of-experiential-networked-intelligence-eni/
140. What is Network Data Analytics Function (NWDAF) in 5G? - 5G HUB TECHNOLOGIES, INC, https://5ghub.us/what-is-network-data-analytics-function-nwdaf-in-5g/
141. Nokia AVA NWDAF - Network Data Analytics Function, https://www.nokia.com/ai-and-analytics/nwdaf/
142. Network Data Analytics Function (NWDAF) - 5G | ShareTechnote, https://www.sharetechnote.com/html/5G/5G_NWDAF.html
143. Oracle Communications Network Data Analytics Function (OC-NWDAF), https://www.oracle.com/a/ocom/docs/industries/communications/comm-network-data-analytics-ds.pdf
144. 5G network data analytics function (NWDAF) - Ericsson, https://www.ericsson.com/en/core-network/5g-core/network-data-analytics-function
145. How to Secure 5G Networks with AI, Zero Trust, and SASE | CXOTalk, https://www.cxotalk.com/episode/how-to-secure-5g-networks-with-ai-zero-trust-and-sase
146. Zero-trust security architecture in the ai era: a novel framework for enterprise cyber resilience, https://ijsra.net/sites/default/files/IJSRA-2024-0172.pdf
147. 5G network AI models: Threats and Mitigations - Check Point Blog, https://blog.checkpoint.com/artificial-intelligence/5g-network-ai-models-threats-and-mitigations/
148. Palo Alto Networks unveils AI-powered zero trust solution to secure 5G networks, https://www.edgeir.com/palo-alto-networks-unveils-ai-powered-zero-trust-solution-to-secure-5g-networks-20250318
149. System Architecture for the 5G System - StandICT.eu, https://2020.standict.eu/standards-watch/system-architecture-5g-system
150. ENISA: 5G design and architecture of global mobile networks; threats, risks, vulnerabilities; cybersecurity considerations - PMC - PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC10446063/
151. Building Mission-Driven 5G Security with Zero Trust - Booz Allen, https://www.boozallen.com/insights/cyber/building-mission-driven-5g-security-with-zero-trust.html