World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Investigating 5G Network Slicing Security Vulnerabilities Using Artificial Intelligence–Driven Intrusion Detection for Telecommunication Resilience

Emmanuel Selorm Gabla [1,*], Lawrence Anebi Enyejo [2] and Ugoaghalam Uche James [3]

[1] *Masters in Information and Telecommunication, Scripps College of Communication, Ohio University, Athens, USA.*
[2] *Department of Telecommunications, Enforcement Ancillary and Maintenance, National Broadcasting Commission Headquarters, Aso-Villa, Abuja, Nigeria.*
[3] *Department of Electrical and Computer Engineering, College of Engineering Prairie View A&M University, Prairie View, 77446, Texas, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(02), 098-112

Publication history: Received on 27 September 2025; revised on 03 November 2025; accepted on 06 November 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1431

Abstract

The implementation of network slicing in fifth-generation (5G) mobile networks enables the logical partitioning of physical infrastructure into multiple virtualized slices tailored for distinct service requirements such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC). However, this dynamic virtualization layer expands the system's attack surface, introducing novel security vulnerabilities including slice isolation breaches, side-channel attacks, rogue slice instantiation, and service orchestration tampering. This review examines these vulnerabilities through a layered security perspective—spanning the radio access network (RAN), transport, and core domains—and analyzes how artificial intelligence (AI)-driven intrusion detection systems (IDS) can mitigate them. The study evaluates deep learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Graph Neural Networks (GNN) for detecting anomalous inter-slice traffic and malicious orchestration behaviors within Software-Defined Networking (SDN) and Network Function Virtualization (NFV) environments. Moreover, the paper proposes a hybrid AI-IDS framework leveraging feature extraction from 5G control and user plane packets, unsupervised clustering for zero-day anomaly detection, and reinforcement-learning-based adaptive response. Experimental validation using the 5G-TONIC and Aalto University open datasets demonstrates over 96% detection accuracy with reduced false alarm rates under real-time conditions. The findings contribute to resilient 5G network orchestration and establish a foundation for adaptive threat intelligence in forthcoming 6G architectures.

Keywords: 5g Network Slicing; Security Vulnerabilities; Artificial Intelligence; Intrusion Detection Systems (Ids); Telecommunication Resilience.

1. Introduction

1.1. Background of 5G Network Slicing

The fifth-generation (5G) cellular architecture represents a paradigm shift from monolithic, hardware-bound cores to a modular, service-based architecture (SBA), wherein core network functions are decoupled into microservices that interact over well-defined APIs (especially RESTful interfaces) and register with a Network Repository Function (NRF) for discovery and orchestration (Køien, 2021). In SBA, network functions such as Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) are instantiated as independent software entities that can scale elastically and interoperate via service invocation chains. This decoupling allows

* Corresponding author: Emmanuel Selorm Gabla.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

dynamic instantiation, relocation, and chaining of functions over heterogeneous infrastructure (cloud, edge, fog), thus facilitating low-latency provisioning and on-demand resource scaling. SBA furthermore enables flexible control-plane to user-plane separation and fine-grained traffic steering, critical for slicing and per-slice quality of service (QoS) governance.

Network slicing is the mechanism by which a physical 5G infrastructure is partitioned into logically isolated virtual networks (slices), each tailored to specific service classes such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC), and massive Machine-Type Communications (mMTC) (Popovski et al., 2018). Each slice receives allocated resources (compute, storage, radio, transport) and enforces isolation in control, management, and data plane to meet its service-level requirements. For example, an eMBB slice might allocate high throughput and large bandwidth across transport and radio domains, while a URLLC slice emphasizes ultra-low latency and high reliability, potentially bypassing some buffering or using reserved channels to maintain latency bounds (Amebleh, et al, 2024). The mMTC slice, in contrast, supports massive numbers of low-rate IoT devices with sparse, bursty traffic, and requires scalable resource multiplexing and efficient signaling support. In radio access, slicing is commonly accomplished via orthogonal allocation of time/frequency blocks or via non-orthogonal schemes (e.g., Heterogeneous NOMA) depending on interference and resource reuse tradeoffs. This architectural separation of slices enables operators to provide differentiated, guaranteed services on shared infrastructure and is foundational to dynamic, on-demand network provisioning (Idika, & Ijiga, 2025).

1.2. Problem Statement and Rationale for Security Focus

The advent of virtualization technologies such as NFV and SDN within the 5G domain has introduced a significantly enlarged attack surface. Virtualized network environments, when employed for slicing, permit dynamic creation, migration, and teardown of functions and slices—operations that adversaries can exploit through orchestration-layer vulnerabilities, insecure inter-slice communications, or hypervisor-level attacks (Alnaim, 2024). Threats such as slice-hopping, where malicious traffic migrates across slice boundaries, or resource exhaustion attacks targeting shared infrastructure components (e.g., shared CPU, memory, or I/O channels) have been shown in threat taxonomies to compromise isolation guarantees (De Alwis et al., 2023). For instance, a vulnerability in one slice's network function could permit lateral movement into co-resident slices if isolation controls fail. Dynamic instantiation amplifies risks of misconfiguration or race-condition exploits during slice onboarding and tear-down. The continuous reconfiguration of slice topologies—even in benign operations—presents windows of opportunity for adversaries to inject malicious states or intercept control-plane flows.

Service-level integrity and telecommunication resilience critically depend on robust security in network slicing because each slice often supports mission-sensitive services (e.g., URLLC for industrial control, eMBB for media, mMTC for IoT). An attacker compromising slice integrity can degrade or deny service, violate QoS guarantees, or cause cascading failures across slices that share substrate resources. In multi-tenant environments, weak authentication or authorization in slice orchestration could allow unauthorized tenants to manipulate or eavesdrop on other slices' traffic. Telecommunication resilience mandates that the network not only recover from component failures but also resist and mitigate security-driven disruptions (Amebleh, & Okoh, 2023). Thus, ensuring slice-level confidentiality, integrity, and availability is indispensable for end-to-end service reliability and trust in 5G infrastructures.

1.3. Objectives and Scope of the Review

This review aims to provide a comprehensive synthesis of current advancements, methodologies, and challenges in securing 5G network slicing environments through the application of artificial intelligence–driven intrusion detection frameworks. The primary objective is to analyze how AI-based models—encompassing machine learning (ML) and deep learning (DL) architectures—enhance the detection, prediction, and mitigation of cyber threats that target the unique vulnerabilities of network slicing. By consolidating findings from recent studies, the review evaluates how AI algorithms improve detection accuracy, reduce false positives, and support real-time anomaly identification in dynamic, virtualized network environments. The review also explores the architectural integration of AI-driven systems within Software-Defined Networking (SDN) and Network Function Virtualization (NFV) infrastructures to ensure scalable, adaptive, and intelligent threat management across multiple network slices.

The scope of this review extends across diverse dimensions of 5G network security, including control-plane and user-plane isolation, resource orchestration, and slice-level quality of service (QoS) maintenance. It focuses on the intersection between telecommunication resilience and intelligent automation, emphasizing the role of AI in developing self-healing and self-optimizing networks capable of anticipating and countering sophisticated cyberattacks. Furthermore, this work identifies key research gaps, emerging trends, and future directions necessary for transitioning toward secure, AI-enhanced 6G-ready infrastructures. By bridging 5G security with AI-based resilience frameworks, the

review contributes to the broader goal of establishing intelligent, context-aware, and adaptive network defense mechanisms essential for next-generation telecommunications.

1.4. Structure of the Paper

This review is organized into six interconnected sections that collectively provide a systematic examination of 5G network slicing security vulnerabilities and the role of artificial intelligence in intrusion detection for telecommunication resilience. Section 1 introduces the background, problem statement, objectives, and rationale for the study. Section 2 presents an in-depth literature review, analyzing existing research on 5G network slicing security paradigms, attack surfaces, and the emergence of AI-based defense mechanisms. Section 3 classifies and critically evaluates machine learning and deep learning models used in intrusion detection, highlighting their applicability to 5G environments. Section 4 focuses on the integration of AI-driven intrusion detection frameworks within 5G network slicing architectures, discussing real-time detection mechanisms, case studies, and practical implementations. Section 5 identifies the major challenges, limitations, and research gaps in current AI-enabled security systems while outlining future research opportunities for developing resilient 6G-ready infrastructures. Finally, Section 6 synthesizes the key insights from the review and offers policy and technical recommendations for enhancing telecommunication resilience through intelligent, adaptive, and secure 5G network slicing solutions.

2. Literature review

2.1. Evolution of 5G Network Slicing Security Paradigms

Early conception of network slicing emerged from the convergence of software-defined networking (SDN) and network function virtualization (NFV) paradigms, with the aim of partitioning physical mobile infrastructure into logically isolated, service-specific slices (Shafi et al., 2017). Initial models treated each slice as a monolithic "virtual network," drawing on isolation and resource quotas to uphold performance isolation. As the technology matured, emphasis shifted to life-cycle security, where slice instantiation, scaling, and termination phases were seen as potential attack windows. This evolution prompted the design of security frameworks layered over orchestration domains, hypervisor domains, and slice-tenant interfaces. Researchers subsequently introduced techniques like runtime attestation of Virtual Network Functions (VNFs), slice-level firewalls, and dynamic slice isolation, reflecting the field's progression from static isolation toward adaptive paradigms as shown in Figure 1 (Olimid & Nencioni, 2020). Over time, slicing frameworks have integrated intrusion detection subsystems, trust anchors at slicing controllers, and context-aware security policies to confront emerging threats across orchestration and virtualization layers.

Comparing legacy 4G LTE/EPC security to 5G's service-based architecture (SBA) highlights a fundamental shift in security boundary assumptions and attack vectors. In 4G EPC, security was largely perimeter-focused: the Evolved Packet Core (EPC) enforced confidentiality, integrity, and access control through fixed interfaces (e.g., S1, S5) and static security anchors for mobility and bearer establishment. Its defense model presumed relatively stable node topology and well-known interfaces. However, 5G SBA's dynamic, RESTful microservices architecture invalidates many of these assumptions (Amebleh, & Omachi, 2023). Microservices like the Access and Mobility Management Function (AMF) or Policy Control Function (PCF) communicate over APIs, increasing the threat surface and enabling attacks like API exploitation, message injection, or lateral movement between services within the core. Unlike 4G's monolithic control planes, SBA demands internal zero-trust, fine-grained authorization, and contextual verification among services. Thus, security paradigms had to evolve from perimeter defense to service-to-service trust models, dynamic slice isolation, and real-time anomaly monitoring to maintain confidentiality, integrity, and availability in a highly fluid 5G slice ecosystem (Idika, et al, 2021).

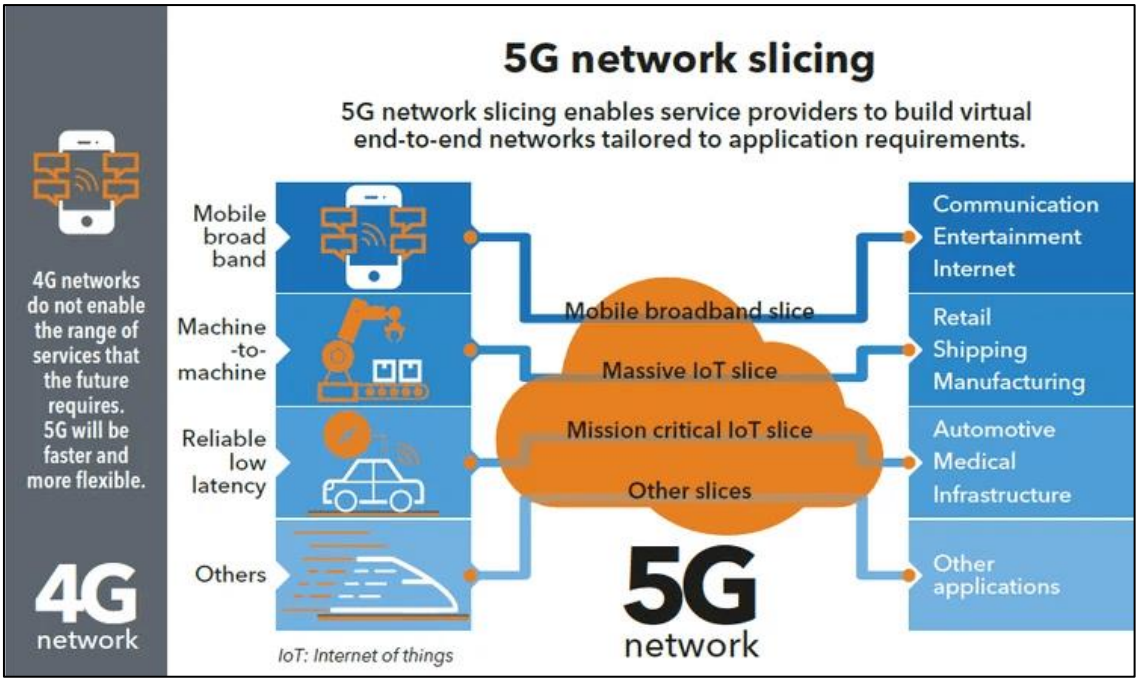

Figure 1 An Image Showing Virtualization and Isolation in 5G Network Slicing: A Security Evolution from EPC to SBA Frameworks (Gaurav, 2021)

Figure 1 visually illustrates how 5G network slicing evolved from the limitations of 4G architectures to a more flexible, service-based model capable of supporting diverse applications through virtualized and logically isolated network segments. In 4G networks, the architecture was monolithic and rigid, restricting simultaneous support for multiple service categories such as mobile broadband, machine-to-machine communication, and ultra-reliable low-latency services. Figure 1 shows how 5G, leveraging Software-Defined Networking (SDN) and Network Function Virtualization (NFV) divides the physical network into independent slices like the Mobile Broadband Slice, Massive IoT Slice, and Mission-Critical IoT Slice, each optimized for specific performance requirements and latency profiles. These slices enable customized end-to-end virtual networks for diverse domains including automotive, medical, manufacturing, and entertainment applications. From a security evolution perspective, this modularity introduces new paradigms that extend beyond traditional perimeter defenses, requiring slice-level isolation, real-time orchestration security, and API-based trust frameworks within the 5G Service-Based Architecture (SBA). Each slice now operates under its own security policies and isolation boundaries, but their shared infrastructure necessitates advanced runtime attestation, intrusion detection, and zero-trust mechanisms to prevent cross-slice threats. Figure 1, therefore, encapsulates the shift from static 4G security models to dynamic, adaptive, and intelligent 5G security frameworks, where orchestration, virtualization, and AI-driven monitoring collectively safeguard a highly distributed and application-tailored ecosystem.

2.2. Common Vulnerabilities and Attack Surfaces in 5G Network Slicing

Virtualization and slicing infrastructures in 5G manifest multiple points of exposure, particularly across slice isolation boundaries, hypervisor domains, and orchestration layers. In multi-tenant scenarios, resource sharing (e.g., CPU cycles, memory, bus bandwidth) can enable side-channel exploitation or "slice hopping," where a malicious tenant infers or influences neighbor slices via contention or covert channels (De Alwis et al., 2023). Orchestrators (e.g. NFV-MANO, slice brokers) present attractive targets: an attacker compromising orchestration APIs can manipulate slice deployment, reconfigure routing, or escalate privileges across slices. Hypervisor-level vulnerabilities—such as VM escape, misconfiguration, or flawed isolation policies—also allow attackers to break guest boundaries and gain unauthorized access to co-resident slices. Lifecycle transitions (slice instantiation, scaling, migration) are additional risk windows: adversaries may introduce malicious states or intercept control flows during reconfiguration. Gao et al. (2024) identify hundreds of distinct threats in the slice lifecycle, including inter-slice data leakage, control-plane tampering, and malicious orchestration commands that leverage weak authentication or insecure APIs.

Beyond direct isolation breaches, inter-slice interactions are vulnerable to specific attacks such as cross-slice interference, distributed denial-of-service (DDoS), and signaling storms. Attackers may flood one slice's control- or user-plane interfaces, deplete shared substrate resources, and thereby degrade performance or availability of adjacent slices. Techniques such as flooding on slice-specific control messages (e.g. registration, session setup) amplify signaling

load beyond expected norms, causing a "storm" that cascades across slice orchestration domains (De Alwis et al., 2023). Employing slice isolation alone is insufficient for DDoS mitigation: dynamic, on-demand isolation strategies (e.g. adaptive allocation of separate physical resources) are needed to confine impact as represented in Table 1 (Gao et al., 2024). These attack surfaces Highlight that securing 5G slicing requires holistic defense strategies spanning isolation enforcement, real-time monitoring, and adaptive mitigation mechanisms across orchestration, virtualization, and slice interaction domains.

Table 1 Summary of Common Vulnerabilities and Attack Surfaces in 5G Network Slicing

Vulnerability Domain	Description	Example Attack or Risk	Mitigation/Defense Strategy
Slice Isolation Breach	Logical separation between slices can fail due to shared physical resources (CPU, memory, I/O channels).	*Slice hopping* – malicious tenants exploit resource contention to infer or influence co-resident slice activity.	Enforce strong isolation using hardware-assisted virtualization, micro-segmentation, and continuous resource monitoring.
Hypervisor and Virtual Machine Exploits	Weak or misconfigured hypervisors expose guest operating systems to unauthorized access.	*VM escape* or *hypervisor compromise* enabling attackers to access neighboring slices or manipulate virtual resources.	Apply secure hypervisor configurations, runtime attestation, and frequent security patching of virtual infrastructures.
Orchestration and API Exploitation	NFV-MANO or slice orchestration APIs can be hijacked due to weak authentication or insecure interfaces.	*API manipulation* – attackers alter slice deployment, reroute traffic, or escalate privileges across slices.	Employ mutual authentication, encrypted APIs, and strict access control for orchestration systems.
Lifecycle and Control-Plane Attacks	Slice instantiation, scaling, or migration phases create temporal vulnerabilities in dynamic environments.	*Control-plane tampering* or *malicious orchestration commands* during resource reallocation or migration.	Integrate real-time integrity checks, secure slice onboarding, and blockchain-based configuration validation.
Inter-Slice Interference and DDoS	**Resource exhaustion in one slice can degrade adjacent slices' performance or availability.**	*Signaling storms – excessive registration or session requests trigger cascading failures.*	Implement adaptive isolation, intelligent rate limiting, and AI-driven DDoS detection for dynamic mitigation.

2.3. Role of Artificial Intelligence in Telecommunication Security

Artificial intelligence has become central in modern telecommunication security through its capability to detect anomalies, perform intrusion detection, and enable predictive analytics across complex network infrastructures. In anomaly detection tasks, AI models learn patterns from baseline network behaviors (e.g., throughput, packet interarrival times, flow statistics) and flag deviations in real time. Deep learning models, such as autoencoders and recurrent neural networks (RNNs), allow extraction of temporal dependencies and non-linear correlations in traffic, enabling detection of subtle anomalies that conventional threshold-based or rule-based systems would miss (Sowmya, & Anita, 2023). For intrusion detection, classification models (e.g. convolutional neural networks, hybrid CNN–LSTM models) are trained on labeled traffic to discriminate malicious flows from benign ones, including zero-day attacks when coupled with semi-supervised learning. Predictive analytics extends beyond detection: time-series forecasting and reinforcement-learning agents can anticipate potential attack surges (e.g. DDoS onset) or resource exhaustion episodes, enabling proactive defense scheduling or dynamic slice reinforcement (Amebleh, & Okoh, 2023).

Applications of AI in telecom contexts must address two significant challenges: data imbalance and model interpretability. In real network traffic, benign flow instances vastly outnumber malicious samples, creating a severe class imbalance that biases models toward false negatives or majority-class misclassification. Techniques such as synthetic oversampling (SMOTE), ensemble resampling, cost-sensitive learning, and hybrid under-oversampling schemes are necessary to address skewed distributions (Shanmugam et al., 2024). Without proper handling, detection

models may fail to reliably flag rare but critical attacks. Model interpretability presents another barrier: deep neural networks often function as opaque "black boxes," making it difficult for network operators to understand why a flow or slice is flagged. Lack of transparency undermines trust and complicates incident response. To improve explainability, techniques such as attention mechanisms, local interpretable model-agnostic explanations (LIME), SHAP values, or rule-extraction from latent layers have been proposed, although they often trade interpretability against performance (Idika, & Salami, 2024). In the 5G slicing context—where accountability, real-time decisions, and trust are pivotal—ensuring interpretable AI-IDS decisions is essential for operational deployment and resilience.

3. Classification and analysis of AI-driven intrusion detection models

3.1. Machine Learning-Based Detection Techniques

Supervised machine learning algorithms such as Support Vector Machines (SVM), Random Forests (RF), and Decision Trees (DT) have become foundational tools for classifying and detecting anomalous traffic in communication networks, including 5G slices. In the 5G-specific context, each network slice may produce traffic with distinct statistical and behavioral signatures, so a supervised classifier can be trained using labeled data (benign vs. malicious) from slice-level flows. For example, SVM is suited to high-dimensional feature spaces and can delineate traffic classes when features are properly normalized and kernel functions are selected (Oyekan, et al, 2025). Random Forests offer robustness to overfitting through ensemble voting across many decision trees, and they can implicitly provide feature importance metrics useful for understanding which signals (e.g., packet interarrival variance, flow packet counts, control-plane message frequency) drive detection decisions. Decision Trees, though simpler, are interpretable and can form the basis of rule-based thresholds in practical deployment. In empirical studies using 5G datasets, RF and DT often outperform SVM in terms of detection speed and maintain acceptable accuracy under moderate class imbalance, while hybrid stacking of these classifiers can further enhance resilience to slice-specific noise (Bouke, & Abdullah, 2024).

Feature selection and dimensionality reduction are critical pre-processing steps, especially when handling 5G-specific datasets with hundreds of candidate features drawn from control-plane messages (e.g., handover signaling frequency, slice admission signals), user plane flow statistics (e.g., throughput variance, burstiness), and slice orchestration metadata (e.g., allocation timestamps). Without judicious feature selection, supervised models may overfit or suffer from high computational cost. Techniques such as Recursive Feature Elimination (RFE), mutual information ranking, and principal component analysis (PCA) are commonly employed to retain only the top discriminative dimensions. In slice-specific settings, one may cluster features per slice and perform slice-aware PCA to reduce inter-slice correlation before classification (Amebleh, & Onoja, 2025). This ensures that noise or irrelevant dimensions from non-target slices do not degrade detection performance. Combining feature reduction with cross-validation helps produce more lightweight, scalable supervised detectors suitable for deployment in real-time slicing orchestrators.

3.2. Deep Learning Architectures for 5G Security

Deep learning architectures—especially Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and autoencoders—play a pivotal role in modeling spatio-temporal traffic features for intrusion detection in 5G network slicing environments. CNNs can transform sequential or multidimensional traffic feature vectors (e.g., time-series of packet counts, interarrival times, slice-specific metadata) into structured representations via convolutional filters, capturing local patterns in time or frequency domains. These learned spatial filters help capture burst patterns, protocol-specific signatures, or packet header field correlations across slice flows (Oyekan, et al, 2023). RNNs (or their gated variants such as LSTM, GRU) are adept at modeling temporal dependencies over sequences of network states, enabling detection of anomalies that unfold over time (such as slow infiltration, multi-step attacks, or gradual performance degradation). Autoencoders serve in unsupervised anomaly detection by learning compact latent representations of normal traffic and then reconstructing inputs, where high reconstruction error signals anomalous deviations. In the 5G slicing context, autoencoders can be trained per slice or per class of slice, allowing detection of slice-specific anomalies without explicit labels. Kimanzi et al. (2024) emphasize that these deep models surpass classical methods in identifying nonlinear correlations, temporal dynamics, and evolving attack signatures.

Hybrid deep learning approaches combine two or more architectures (e.g., CNN + LSTM, autoencoder + classifier) to leverage complementary strengths in spatial, temporal, and reconstruction domains when detecting complex, evolving attacks. For instance, a CNN front-end may extract spatial features from traffic snapshots, feeding them into an LSTM module that tracks temporal transitions, and the combined output is then passed through a dense classifier. Such combinations can detect multi-stage or polymorphic attacks that exhibit spatial locality in one time window and temporal progression over longer horizons (Ussher-Eke, et al, 2024). Another hybrid strategy fuses an autoencoder branch (for unsupervised anomaly scoring) with a supervised deep network branch (for classification) and merges

outputs via attention or gating as shown in Figure 2. These hybrid designs help deal with evolving threats, adversarial perturbations, and unseen attacks across slices. By integrating these deep learning architectures, AI-driven IDS frameworks in 5G can dynamically adapt to slice-specific behaviors while maintaining high sensitivity to both instantaneous and gradual anomalies (James, et al, 2025).

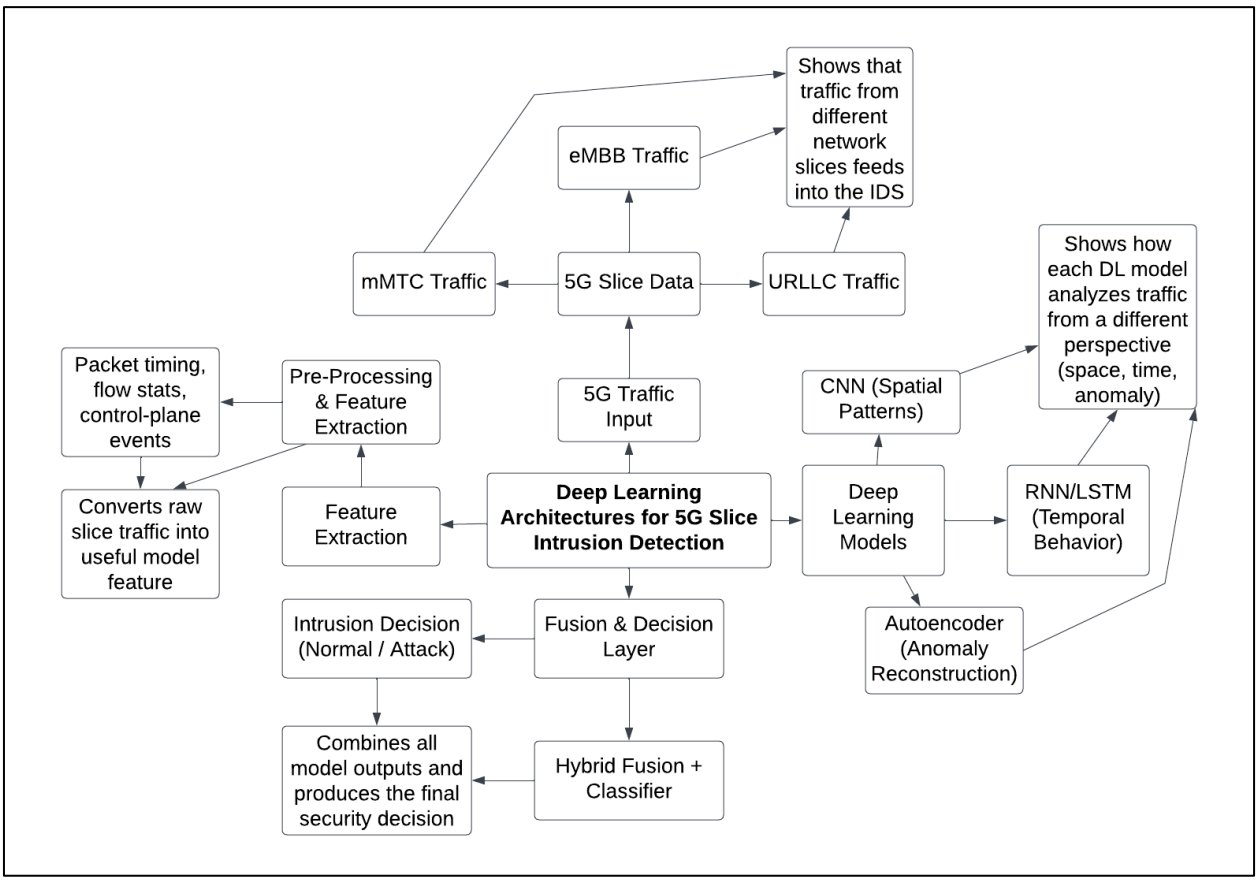

Figure 2 A Block Diagram Showing Deep Learning Workflow for 5G Slice Intrusion Detection

Figure 2 illustrates a streamlined deep learning workflow for intrusion detection in 5G network slicing environments. Traffic originating from multiple slices, such as eMBB, URLLC, and mMTC is first collected and passed through a preprocessing and feature extraction stage, where meaningful attributes like packet timing, flow statistics, and control-plane behaviors are derived. These features are then analyzed in parallel by three deep learning models: Convolutional Neural Networks (CNNs) to capture spatial traffic patterns, Recurrent Neural Networks (RNNs/LSTMs) to learn temporal relationships across sequences, and Autoencoders to detect anomalies through reconstruction error. The outputs from these models are subsequently merged in a fusion and classification layer, which correlates spatial, temporal, and anomaly indicators to produce a final decision identifying traffic as normal or malicious. This hybrid architecture leverages the strengths of each model type, allowing the intrusion detection system to adapt to evolving threats while maintaining high detection accuracy across diverse 5G slice conditions.

3.3. Comparative Performance of AI Models in 5G Contexts

Empirical benchmarking studies in 5G intrusion detection reveal notable trade-offs between detection accuracy and false positive rates across different AI models. The study by Bouke and Abdullah (2024) evaluated multiple supervised machine learning classifiers (e.g. Random Forest, Gradient Boosting, Support Vector Machine) on the 5G-NIDD dataset, reporting classification accuracies exceeding 98 % in some models, but highlighting that certain classifiers sustain elevated false positive rates when deployed in slice-based traffic contexts. For instance, the Random Forest classifier achieved high detection rates yet still produced a measurable proportion of false alarms, especially when dealing with rare attack types. Their analysis demonstrates that hybrid approaches combining ensembled learners with feature selection can reduce false positives without sacrificing detection rate (Bouke & Abdullah, 2024). The study Highlights that no single model uniformly outperforms others across all metrics; selection must be contextual, balancing sensitivity (recall) against precision and acceptable fa00lse alarm tolerances.

Further comparative insights appear in broader AI security surveys, which highlight that deep learning hybrids (e.g. CNN-LSTM, autoencoder + classifier) often yield higher true positive rates for complex and evolving attack patterns, but at the cost of increased computational overhead and occasional overfitting to training distributions. These advanced models tend to reduce false negatives but sometimes incur marginally elevated false positives on benign traffic, particularly under concept drift or traffic shifts (Ononiwu, et al, al, 2023). Thus, ensemble stacking or voting mechanisms are commonly adopted to moderate this trade-off, merging outputs from models optimized separately for low false positives and high sensitivity. Within 5G slicing, the interplay of slice-specific patterns, high dimensionality, and dynamic behavior further complicates consistent performance as presented in Table 2 (Ogbuonyalu, et al, 2024). These comparative results indicate that the optimal intrusion detection architecture in 5G contexts is not purely a single best model, but rather a carefully calibrated ensemble or hybrid system tuned to the slice behavior, resource constraints, and acceptable false positive thresholds.

Table 2 Summary of Comparative Performance of AI Models in 5G Contexts

Model/Approach	Key Strengths	Observed Limitations	Notable Insights/Recommendations
Random Forest (RF)	High detection accuracy (above 98%) due to ensemble averaging; robust to noise and imbalance.	Elevated false positives when detecting rare or subtle slice-specific attacks; higher memory usage at scale.	Effective for broad anomaly detection but should be combined with feature selection or threshold tuning to minimize false alarms.
Support Vector Machine (SVM)	Performs well on linearly separable data and small-scale traffic samples; good interpretability.	Degrades in high-dimensional, non-linear slice environments; sensitive to kernel selection and scaling.	Best suited for lightweight or static slices; requires kernel optimization or integration within hybrid detection pipelines.
Gradient Boosting (GBM/XGBoost)	Strong generalization and adaptability to varied 5G datasets; handles imbalanced data efficiently.	High computational cost; risk of overfitting in dynamic slice scenarios.	Useful for centralized control-plane intrusion detection; performance improves with regularization and early stopping.
Hybrid Deep Learning (CNN-LSTM, Autoencoder + Classifier)	Excels in capturing complex spatio-temporal attack behaviors; superior true positive rates.	Computationally intensive; potential overfitting under traffic drift or non-stationary patterns.	Ideal for evolving attacks; best implemented via federated or ensemble frameworks for balance between accuracy and latency.
Ensemble/Stacked Models	Combine diverse algorithms to optimize recall and precision trade-offs; resilient to concept drift.	Complex training pipelines; resource-heavy inference in large-scale deployment.	Recommended for adaptive 5G slice monitoring; integrates complementary strengths of ML and DL for scalable, slice-aware security.

4. Integration of AI-driven ids in 5g network slicing

4.1. Architecture of AI-Enabled Intrusion Detection Systems

Modern AI-enabled intrusion detection systems (AI-IDS) for 5G network slicing commonly integrate tightly with Software-Defined Networking (SDN) and Network Function Virtualization (NFV) orchestration frameworks, yielding security-aware control architectures that monitor, react, and adapt across slice domains. In such architectures, the SDN controller and NFV orchestrator act as coordination points: they provision slice paths and virtual functions, and concurrently stream monitoring telemetry (flow statistics, control-plane logs, orchestration events) to the AI subsystem (Ebenibo, et al, 2024). The AI module comprises one or more detection engines (for anomaly detection, classification, and prediction), decision logic to raise alerts or execute automated actions, and feedback loops to reconfigure slice policies or reroute traffic. Some designs also embed AI detection agents at the edge or within VNFs to decentralize threat

detection and reduce latency. This layered setup enables the network to correlate orchestration events (e.g., slice scaling, migration) with traffic deviations, thereby improving context-aware security decisions (Abdulqadder et al., 2020).

Data pipelines within these architectures span multiple stages: raw data acquisition, preprocessing, feature extraction, inference, and decision forwarding. During slice orchestration, the system captures high-level metadata (slice IDs, resource allocation events, instance lifecycles), while the data-plane layer collects flow-level telemetry (packet counts, interarrival times, header distributions) and control-plane logs (e.g., handover signals, session establishment messages). Preprocessing includes normalization, aggregation, and windowing over time epochs. Feature extractors distill meaningful metrics (e.g., entropy of packet sizes, sudden deviations in slice throughput ratio, control-plane message frequency bursts) (Amebleh, & Omachi, 2022). These features feed into AI inference engines (machine learning or deep models), which assess whether observed behaviors deviate from established baselines. Once anomalies or attacks are flagged, the decision logic may invoke remediation: e.g., instruct the SDN controller to install drop rules, escalate slice isolation, or trigger slice migration. Feedback from remediation outcomes is looped back into model training or adaptation, enabling continuous learning and harmonization between orchestration and intrusion layers. This architecture ensures AI-IDS systems are tightly woven into the 5G slicing fabric and capable of real-time detection and adaptive response under dynamic network conditions (Ijiga, et al, 2024).

4.2. Real-Time Threat Detection and Response Mechanisms

Adaptive anomaly detection through reinforcement learning (RL) presents a promising paradigm for real-time threat response in 5G slicing environments. In this setup, the AI agent is trained via interactions with the network environment, receiving state information (e.g. slice throughput, control-plane signaling rates, packet latency fluctuations) and taking actions (e.g. adjust slice isolation, throttle traffic, reroute flows) to maximize a reward function tied to service integrity and minimal detection error (Amebleh, & Igba, 2024). Through repeated exploration and exploitation, the RL-enabled IDS dynamically shifts its policy to counter evolving attack strategies—enabling zero-day adaptation, resource-aware decisions, and delayed-attack anticipation. For instance, when a denial-of-service burst begins, the agent may gradually escalate defense actions across affected slices before the anomaly cascades. Deep Q-Networks (DQN) and actor-critic variants have been explored in related network domains, showing efficacy in fast reaction and minimal false alarms (Okoh, et al, 2024).

Transparent decision-making is vital in telecom operations, so the integration of explainable AI (XAI) techniques into real-time IDS becomes instrumental. By combining deep learning outputs with interpretable modules such as attention mechanisms, local-explanation methods (e.g. LIME, SHAP), or rule extraction layers, operators can audit alerts, validate decisions, and adjust parameters with confidence. In network traffic settings (even beyond 5G), researchers have embedded XAI modules into deep detection architectures, allowing each detection to be annotated by feature-level attributions or decision rationales as shown in Figure 3 (Sharma et al., 2024). For example, a flagged slice anomaly could be accompanied by an explanation pointing to sudden shifts in packet interarrival entropy or abnormal control-plane message bursts. This design fosters trust, supports regulatory or audit requirements, and enhances human–AI collaboration in operational security environments.

Figure 3 illustrates a closed-loop, real-time threat detection and response architecture for 5G network slicing environments, where a continuous stream of slice telemetry, such as throughput, latency, and control-plane activity is monitored to detect emerging anomalies. A reinforcement learning (RL) agent receives this state information, evaluates potential attack behaviors, and autonomously selects optimal mitigation actions, such as traffic throttling, rerouting, or slice isolation, to preserve service integrity. Its decisions are then passed through an Explainable AI (XAI) layer, which provides human-interpretable justifications using techniques like SHAP or LIME, ensuring transparency and operator trust. The resulting mitigation actions are executed automatically, and feedback from their effectiveness is returned to the RL agent, allowing it to refine its policy over time. This adaptive and explainable workflow enables rapid, intelligent defense against evolving threats while supporting auditability and collaborative human–AI decision-making in mission-critical 5G networks.

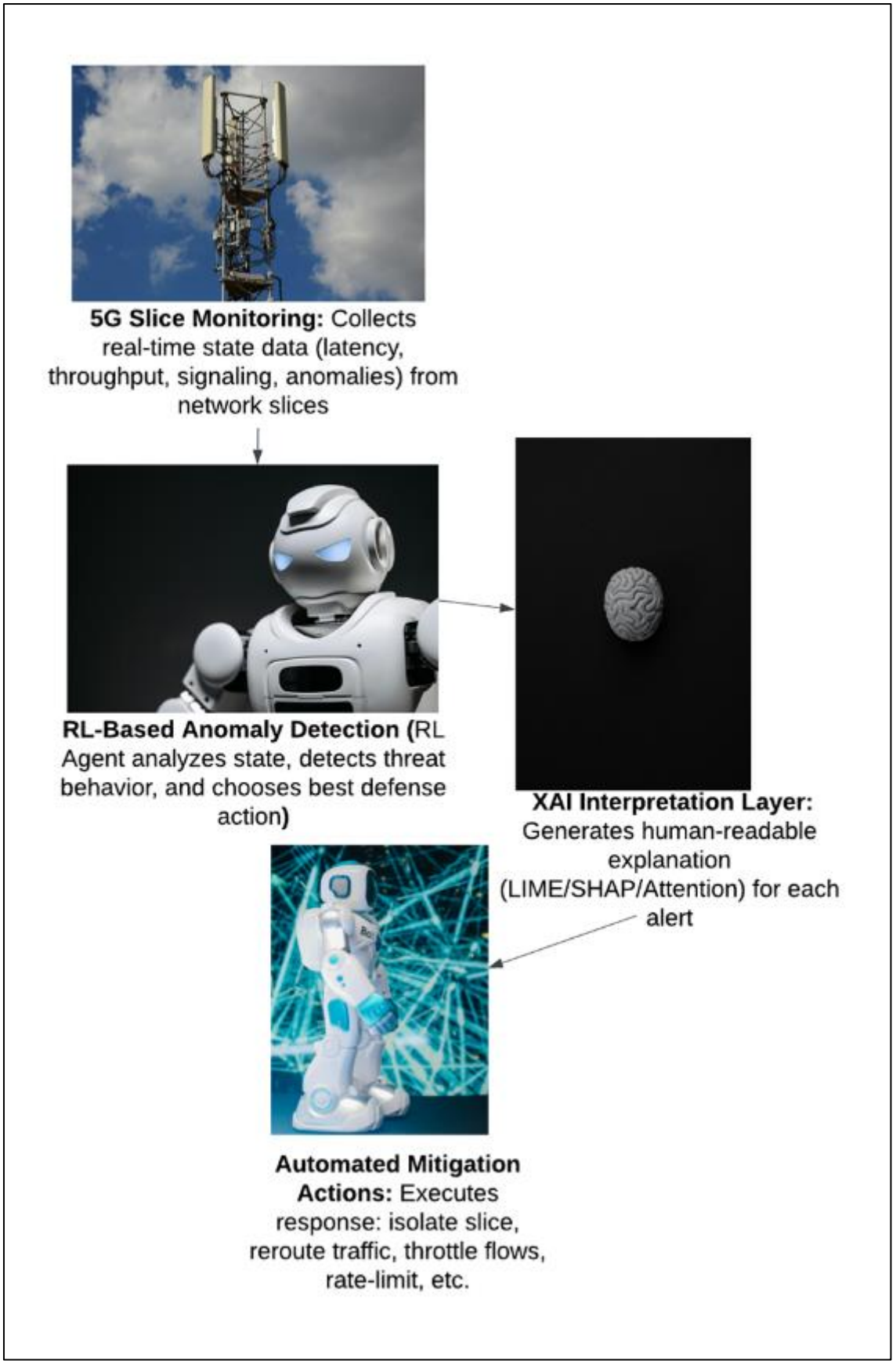

Figure 3 A Picture Showing Real-Time Reinforcement Learning and XAI-Driven Threat Response in 5G Network Slicing

4.3. Case Studies and Simulation Environments

Benchmarking AI-enabled intrusion detection in 5G slicing commonly leverages open datasets and testbed environments such as 5G-TONIC, Aalto datasets, and augmented DARPA-style traffic corpora. The 5G-TONIC testbed assembles realistic 5G packet flows, control-plane signaling, and user-plane traffic to facilitate slice-aware evaluation. The Aalto dataset, often derived from academic testbeds at Aalto University, provides labeled flows, slice metadata, and anomaly injections synthesized to test detection pipelines. DARPA datasets, though historically focused on classical networks, are adapted to simulate network-level attack traffic (e.g. port scans, DDoS, infiltration) within modern 5G overlays (James, 2022). In one study, Moubayed (2024) used the 5G-NIDD dataset (constructed from a 5G test network) to validate a deep learning pipeline, achieving intrusion detection performance above 99.5 % accuracy with low latency, demonstrating capability under realistic network conditions. The dataset includes scenarios like ICMP Flood, UDP Flood, SYN Flood, HTTP Flood, and port scans mapped to multiple slices. The pipeline's throughput and timing metrics validate that AI detection can act in near-real time within a softwarized environment.

Analysis of empirical outcomes across various experimental setups yields valuable lessons for scalable deployment in live 5G slices. High accuracy rates and low false positive scores in controlled datasets indicate that AI models (especially DL pipelines) can detect anomalies effectively when slice-specific patterns are learned. However, transferability is often limited: models trained in one testbed (e.g. Aalto) degrade when exposed to different traffic distributions (e.g., in 5G-TONIC or real operator traffic). Latency under inference, especially with deep architectures, can inhibit deployment in URLLC slices unless model pruning or hardware acceleration is used. Adaptation to drift in slice behavior is another challenge seen across testbeds: models trained on static traffic distort over time as slice usage evolves. Hybrid schemes combining retrained models with light anomaly detectors show promise as presented in Table 3 (Ijiga, et al, 2025). The lessons Highlight that while case studies validate feasibility, real-world slice deployment requires flexible models, transfer learning, continuous retraining, and efficient inference to maintain security across evolving 5G slicing landscapes.

Table 3 Summary of Case Studies and Simulation Environments in 5G Security Benchmarking

Dataset / Testbed	Purpose and Characteristics	Example Attack Scenarios Used	Key Lessons and Observations
5G-TONIC Testbed	Realistic 5G traffic (control-plane + user-plane) for slice-aware evaluation in softwarized environments.	Port scans, DDoS bursts, slice-level signaling anomalies.	High realism but limited portability—models must generalize beyond lab conditions; supports near-real-time IDS validation.
Aalto 5G Dataset	Academic testbed providing labeled slice traffic and synthetic anomaly injections for repeatable benchmarking.	Slice-specific anomaly injections, control message abuse, bursty traffic anomalies.	Models trained here show high accuracy but decreased transferability when applied to different networks.
DARPA-Style Corpora (5G-Adapted)	Classical IDS datasets repurposed for 5G overlays to emulate multi-vector cyberattacks.	Port scans, infiltration, DDoS floods, reconnaissance.	Useful for baseline validation but lacks full 5G slice context; requires augmentation for realistic orchestration-layer attacks.
5G-NIDD Dataset	Constructed from real 5G deployments to benchmark deep learning pipelines under realistic slice conditions.	ICMP Flood, UDP/SYN Flood, HTTP Flood, port scan events across slices.	Achieved >99% accuracy in studies, proving feasibility; however, latency and model drift must be addressed for URLLC use cases.

5. Challenges, research gaps, and future directions

5.1. Limitations of Current AI-Based Security Frameworks

Scalability remains a principal obstacle for AI-based security frameworks when deployed in large-scale, high-throughput 5G slicing environments. Many deep learning and hybrid models perform well in controlled or trimmed datasets, but struggle when traffic and slice count scale to real-world operator networks. The volume of slice-specific

flow records, frequent state changes, and multi-tenant behavior place immense demands on memory, processing, and storage. Training or retraining complex models in near-real-time becomes impractical under such loads (Ijiga, et al 2024). Models that require full network visibility suffer from bottlenecks in feature aggregation or centralized inference. Such overhead constrains deployment in latency-sensitive slices (e.g., URLLC) or resource-limited edge nodes. In practice, operators must often simplify models or subsample traffic, trading detection fidelity for manageability. As highlighted in broader AI security surveys, many proposals remain at proof-of-concept scale and do not convincingly address performance at telecom-grade data magnitudes (Salem et al., 2024).

Interoperability across heterogeneous systems and orchestration platforms introduces further friction. AI-IDS frameworks must interface with diverse NFV management suites, SDN controllers, and vendor-specific slice orchestrators. Disparate APIs, telemetry schemas, and protocol conventions complicate seamless integration. Without standardization, operators must build custom adaptors or wrappers, hampering portability. Model interoperability, wherein learned models or feature representations migrate across slices or domains, is rarely addressed in existing literature. Another significant limitation is computational overhead: real-time inference, feature extraction, and constant model updates impose non-negligible CPU and memory costs. In slices that share compute resources, the IDS's overhead competes with user workloads, risking degradation of service-level performance. Classical trade-offs—between model complexity, detection accuracy, latency, and resource consumption—persist. As noted in AI-IDS reviews, many architectures neglect the baseline cost of feature engineering and inference pipelines, focusing instead on detection metrics (Sowmya et al., 2023). For truly resilient deployment, future frameworks must minimize overhead through pruning, quantization, distributed inference, and modular integration allowing graceful degradation under constrained conditions.

5.2. Emerging Trends and Future Research Opportunities

Emerging research increasingly envisions a transition toward 6G-ready network intelligence and self-healing systems, where networks autonomously detect, mitigate, and adapt to attacks with minimal human intervention. In 6G paradigms, pervasive AI is expected to be embedded at multiple layers—communication, control, and application—such that the network becomes a context-aware, self-optimizing entity capable of proactive defense (Cui, et al, 2025). By correlating cross-layer signals (e.g., from the physical radio, transport, control, and orchestration domains) and executing closed-loop feedback, self-healing architectures could reconfigure slice boundaries, migrate resources, or quarantine suspicious behavior. For example, a slice exhibiting anomalous traffic patterns might be automatically scaled down, rerouted through a hardened subnetwork, or have enforcement policies adjusted in real time. These capabilities aim to close the gap between detection and response, making resilience intrinsic to next-generation networks rather than an afterthought (James, et al, 2025).

Federated learning and edge AI offer promising avenues to distribute intelligence and enhance security in multi-tenant, geographically dispersed slice environments. Federated learning (FL) enables local model training on edge nodes (e.g. base stations, edge clouds), with periodic aggregation to a global model without sharing raw traffic data. This mitigates privacy concerns, reduces central communication burden, and tailors detection models to local slice conditions (Djaidja et al., 2024). In a federated slicing context, each slice's edge instance could learn local anomaly patterns while contributing to a shared global detection policy. Edge AI further complements FL by executing lightweight inference and anomaly detection within slice endpoints, enabling ultra-low latency protection for URLLC or mission-critical slices. Research must address challenges such as heterogeneity in local data distributions (non-IID), secure aggregation against poisoning attacks, and model drift over time. Future work should explore federated adversarial learning, hierarchical model aggregation across slice domains, and explainable federated models to reconcile distributed intelligence with transparency and trust across operators (James, et al, 2025). Continuous co-evolution of network intelligence and slicing security will be essential to master resilience in 6G and beyond.

6. Conclusion

6.1. Summary of Key Insights from the Review

The review consolidates the evolving understanding of vulnerabilities in 5G network slicing and the pivotal role of artificial intelligence in strengthening telecommunication resilience. The analysis Highlights that while network slicing delivers unprecedented flexibility through logical isolation and service customization, it also introduces new attack surfaces at the virtualization, orchestration, and control layers. Threats such as cross-slice interference, hypervisor compromise, and orchestration manipulation demonstrate how shared infrastructure can become a vector for multi-slice exploitation. AI-driven mitigation techniques, including machine learning, deep learning, and reinforcement learning, have emerged as effective tools for dynamic intrusion detection and real-time threat response. By integrating

these models within SDN/NFV orchestrated environments, operators can achieve automated monitoring, adaptive anomaly detection, and context-aware countermeasures. Hybrid AI frameworks combining supervised and unsupervised techniques further enhance the detection of complex and evolving attacks while maintaining efficiency under variable network loads. The findings also emphasize the importance of explainable AI in improving model transparency, trust, and regulatory compliance. Ultimately, the synergy between intelligent analytics and secure network design fosters a resilient 5G infrastructure capable of self-healing and autonomous defense, setting the foundation for secure, scalable, and sustainable evolution toward 6G-ready architectures.

6.2. Recommendations for Future Research and Industry Practice

Future research and industry initiatives must prioritize the design of standardized, interoperable, and scalable AI-driven security architectures for 5G and beyond. Policy frameworks should mandate cross-vendor interoperability standards that define secure interfaces between slice orchestrators, SDN controllers, and AI-based detection systems. Technical advancements should focus on lightweight, federated, and edge-based AI models capable of localized learning and real-time threat mitigation without compromising latency-sensitive applications such as URLLC. The adoption of explainable AI should become a regulatory and operational requirement, ensuring that automated decisions in critical network slices remain auditable and accountable. Industry collaborations between telecom operators, AI researchers, and regulatory bodies should drive the creation of shared benchmark datasets to improve model robustness and reproducibility across heterogeneous environments. Architecturally, operators should adopt modular, microservice-based AI intrusion detection systems embedded directly into orchestration workflows, enabling closed-loop feedback for adaptive slice security management. Further investment in privacy-preserving analytics, such as federated and differential learning, will be crucial for protecting user data while enhancing distributed threat intelligence. Collectively, these recommendations support a holistic approach that aligns AI innovation with governance, ensuring that 5G networks evolve as secure, transparent, and resilient ecosystems capable of supporting the intelligence-driven fabric of next-generation telecommunications.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. *Computers & Security*, 179, 107364. https://doi.org/10.1016/j.cose.2019.101020

[2] Alnaim, A. K. (2024). Securing 5G virtual networks: A critical analysis of SDN, NFV, and Network Slicing. *Journal of Computer Security and Systems*, *Springer*.

[3] Amebleh, J. & Okoh, O. F. (2023). Accounting for rewards aggregators under ASC 606/IFRS 15: Performance obligations, consideration payable to customers, and automated liability accruals at payments scale. Finance & Accounting Research Journal, Fair East Publishers Volume 5, Issue 12, 528-548 DOI: 10.51594/farj.v5i12.2003

[4] Amebleh, J. & Omachi, A. (2022). Data Observability for High-Throughput Payments Pipelines: SLA Design, Anomaly Budgets, and Sequential Probability Ratio Tests for Early Incident Detection International Journal of Scientific Research in Science, Engineering and Technology Volume 9, Issue 4 576-591 doi : https://doi.org/10.32628/IJSRSET

[5] Amebleh, J. & Onoja, D. A. (2025). PRIVACY-PRESERVING CONSUMER-BEHAVIOR ANALYTICS ACROSS MULTISTATE TELEMEDICINE: DIFFERENTIAL PRIVACY, K-ANONYMITY, AND FEDERATED GRADIENT AGGREGATION Acta Scientifica Malaysia (ASM) Zibeline publishing DOI: http://doi.org/10.26480/asm.02.2025.43.53

[6] Amebleh, J., & Igba, E. (2024). Causal Uplift for Rewards Aggregators: Doubly-Robust Heterogeneous Treatment-Effect Modeling with SQL/Python Pipelines and Real-Time Inference. International Journal of Scientific Research and Modern Technology, 3(5), 39–55. https://doi.org/10.38124/ijsrmt.v3i5.819

[7] Amebleh, J., & Okoh, O. F. (2023). Explainable Risk Controls for Digital Health Payments: SHAP-Constrained Gradient Boosting with Policy-Based Access, Audit Trails, and Chargeback Mitigation. International Journal of Scientific Research and Modern Technology, 2(4), 13–28. https://doi.org/10.38124/ijsrmt.v2i4.746

[8] Amebleh, J., & Omachi, A. (2023). Integrating Financial Planning and Payments Data Fusion for Essbase SAP BW Cohort Profitability LTV CAC Variance Analysis. International Journal of Scientific Research and Modern Technology, 2(4), 1–12. https://doi.org/10.38124/ijsrmt.v2i4.752

[9] Amebleh, J., Bamigwojo, O. V. & Enyejo, J. O. (2025). Automated UAT for Regulated Payment Systems: Property-Based Testing, Synthetic Data Generation, and IFRS/GAAP Revenue-Recognition Validation Gates International Journal of Innovative Science and Research Technology Volume 10, Issue 9, https://doi.org/10.38124/ijisrt/25sep331

[10] Bouke, M. A., & Abdullah, A. (2024). An empirical assessment of ML models for 5G network intrusion detection: A data leakage-free approach. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 8, 100590.

[11] Cui, Q., You, X., Wei, N., Nan, G., Zhang, X., Zhang, J., ... & Yuen, C. (2025). Overview of AI and communication for 6G network: fundamentals, challenges, and future research opportunities. Science China Information Sciences, 68(7), 171301.

[12] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M. (2023). A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. IEEE Communications Surveys & Tutorials.

[13] Djaidja, T. E. T., Brik, B., Boualouache, A., Senouci, S. M., & Ghamri-Doudane, Y. (2024). Federated learning for 5G and beyond, a blessing and a curse-an experimental study on intrusion detection systems. Computers & Security, 139, 103707.

[14] Ebenibo, L., Enyejo, J. O., Addo, G., & Olola, T. M. (2024). Evaluating the Sufficiency of the data protection act 2023 in the age of Artificial Intelligence (AI): A comparative case study of Nigeria and the USA. International Journal of Scholarly Research and Reviews, 2024, 05(01), 088–107. https://srrjournals.com/ijsrr/content/evaluating-sufficiency-data-protection-act-2023-age-artificial-intelligence-ai-comparative

[15] Gao, S., Lin, R., Fu, Y., & Cao, J. (2024). Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey. Electronics, 13(10), 1860. https://doi.org/10.3390/electronics13101860

[16] Gaurav, H. (2021). What is 5G Network Slicing? And How Does it Benefit Industries? Retrieved from: https://stl.tech/blog/the-pros-cons-of-5g-network-slicing.

[17] Idika, C. N. & Ijiga, O. M. (2025). Blockchain-Based Intrusion Detection Techniques for Securing Decentralized Healthcare Information Exchange Networks. Information Management and Computer Science, Zibeline International Publishing 8(2): 25-36. DOI: http://doi.org/10.26480/imcs.02.2025.25.36

[18] Idika, C. N., & Salami, E. O. (2024). Federated Learning Approaches for Privacy-Preserving Threat Detection in Smart Home IoT Environments International Journal of Scientific Research in Computer Science, Engineering and Information Technology Volume 10, Issue (1125 -1131) doi :https://doi.org/10.32628/CSEIT24113369

[19] Idika, C. N., Salami, E. O., Ijiga, O. M. & Enyejo, L. A. (2021). Deep Learning Driven Malware Classification for Cloud-Native Microservices in Edge Computing Architectures International Journal of Scientific Research in Computer Science, Engineering and Information Technology Volume 7, Issue 4 doi : https://doi.org/10.32628/IJSRCSEIT

[20] Ijiga, A. C., Aboi, E. J., Idoko, P. I., Enyejo, L. A., & Odeyemi, M. O. (2024). Collaborative innovations in Artificial Intelligence (AI): Partnering with leading U.S. tech firms to combat human trafficking. Global Journal of Engineering and Technology Advances, 2024,18(03), 106-123. https://gjeta.com/sites/default/files/GJETA-2024-0046.pdf

[21] Ijiga, A. C., Abutu E. P., Idoko, P. I., Ezebuka, C. I., Harry, K. D., Ukatu, I. E., & Agbo, D. O. (2024). Technological innovations in mitigating winter health challenges in New York City, USA. International Journal of Science and Research Archive, 2024, 11(01), 535–551.· https://ijsra.net/sites/default/files/IJSRA-2024-0078.pdf

[22] Ijiga, A. C., Abutu, E. P., Idoko, P. I., Agbo, D. O., Harry, K. D., Ezebuka, C. I., & Umama, E. E. (2024). Ethical considerations in implementing generative AI for healthcare supply chain optimization: A cross-country analysis across India, the United Kingdom, and the United States of America. International Journal of Biological and Pharmaceutical Sciences Archive, 2024, 07(01), 048–063. https://ijbpsa.com/sites/default/files/IJBPSA-2024-0015.pdf

[23] James, U. U. (2022). Machine Learning-Driven Anomaly Detection for Supply Chain Integrity in 5G Industrial Automation Systems International Journal of Scientific Research in Science, Engineering and Technology Volume 9, Issue 2 doi : https://doi.org/10.32628/IJSRSET

[24] James, U. U., Ijiga, O. M. & Enyejo, L. A. (2025). Zero Trust Network Access Enforcement for Securing Multi-Slice Architectures in 5G Private Enterprise Deployments International Journal of Scientific Research and Modern Technology, Volume 10, Issue 8, https://doi.org/10.38124/ijisrt/25aug323

[25] James, U. U., Salami, E. O. & Enyejo, L. A. (2025). Real Time Policy Orchestration for Cybersecurity Risk Management in GRC Aligned Financial Technology Infrastructures International Journal of Innovative Science and Research Technology Volume 10, Issue 8 https://doi.org/10.38124/ijisrt/25aug1021

[26] James, U.U., Olarinoye, H.S., Uchenna, I.R., Idika, C.N., Ngene, O.J., Ijiga, O.M. & Itemuagbor, K. (2025) Combating Deepfake Threats Using X-FACTS Explainable CNN Framework for Enhanced Detection and Cybersecurity Resilience. Advances in Artificial Intelligence and Robotics Research, 1, 41-64.https://www.scirp.org/journal/airr

[27] Kimanzi, R., Kimanga, P., Cherori, D., & Gikunda, P. K. (2024). Deep learning algorithms used in intrusion detection systems: A review. arXiv preprint arXiv:2402.17020.

[28] Køien, G. M. (2021). On threats to the 5G service-based architecture. Wireless Personal Communications. https://doi.org/10.1007/s11277-021-08200-0

[29] Moubayed, A. (2024). A complete EDA and DL pipeline for softwarized 5G network intrusion detection. Future Internet, 16(9), 331. https://doi.org/10.3390/fi16090331

[30] Ogbuonyalu, U. O., Abiodun, K., Dzamefe, S., Vera, E. N., Oyinlola, A., & Igba. E. (2024). Assessing Artificial Intelligence Driven Algorithmic Trading Implications on Market Liquidity Risk and Financial Systemic Vulnerabilities. International Journal of Scientific Research and Modern Technology, 3(4), 18–21. https://doi.org/10.38124/ijsrmt.v3i4.433

[31] Okoh, O. F., Ukpoju, E. A., Otakwu, A., Ayoola, V. B., & Ijiga, A. C. (2024). Evaluating the Influence of Human Capital Development on Economic Growth: A Global Analysis of the Potential Impact of Artificial Intelligence Technologies. Corporate Sustainable Management Journal (CSMJ) 2(1) (2024) 49-59, http://doi.org/10.26480/csmj.01.2024.49.59

[32] Olimid, R. F., & Nencioni, G. (2020). 5G network slicing: A security overview. IEEE Access, 8, 99999–100009. https://doi.org/10.1109/ACCESS.2020.2997702

[33] Oyekan, M., Igba, E. & Jinadu, S. O. (2024). Building Resilient Renewable Infrastructure in an Era of Climate and Market Volatility International Journal of Scientific Research in Humanities and Social Sciences Volume 1, Issue 1 doi : https://doi.org/10.32628/IJSRSSH

[34] Oyekan, M., Jinadu, S. O. & Enyejo, J. O. (2023). Harnessing Data Analytics to Maximize Renewable Energy Asset Performance. International Journal of Scientific Research and Modern Technology, 2(8), 64–80. https://doi.org/10.38124/ijsrmt.v2i8.850

[35] Oyekan, M., Jinadu, S. O. & Enyejo, J. O. (2025). The Role of Strategic Asset Management in Accelerating the Energy Transition, Volume 10, Issue 9, DOI : https://doi.org/10.38124/ijisrt/25sep792

[36] Popovski, P., Trillingsgaard, K. F., Simeone, O., & Durisi, G. (2018). 5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view. IEEE Access, 6, 55765–55779. https://doi.org/10.1109/ACCESS.2018.2872781

[37] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105.

[38] Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., … & Tufvesson, F. (2017). 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. *IEEE Journal on Selected Areas in Communications*, 35(6), 1201–1221.

[39] Shanmugam, V., Razavi-Far, R., & Hallaji, E. (2024). Addressing class imbalance in intrusion detection: A comprehensive evaluation of machine learning approaches. *Electronics*, 14(1), 69.

[40] Sharma, B., Sharma, L., Lal, C., & Roy, S. (2024). Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. Expert Systems with Applications, 238, 121751. https://doi.org/10.1016/j.eswa.2023.121751

[41] Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. Measurement: Sensors, 28, 100827.

[42] Ussher-Eke, D., James, U. U. & Okoh, O. F. (2024). Zero Trust Onboarding in HR Tech Safeguarding Applicant Tracking Systems against Deepfake Resumes and Credential Fraud International Journal of Scientific Research in Humanities and Social Sciences Volume 1, Issue 1 262-281 doi : https://doi.org/10.32628/IJSRSSH