SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I8P123

Volume 12 Issue 8, 269-279, August 2025

Original Article

Security Vulnerabilities and AI-Driven Intrusion Detection in 5G Network Slicing Architectures

Guntu Nooka Raju[1], Rebba Sasidhar[2], P Vamsi Sagar[3], Shaik Nannu Saheb[4], N.V.A. Ravi Kumar[5], Vasupalli Manoj[6*]

[1]*Department of ECE, GMR Institute of Technology, Rajam, India.*
[2]*Department of EEE, Avanthi Institute of Engineering and Technology, Cherukupally, Vizianagaram, India.*
[3]*Department of Mathematics, Aditya University, Surampalem, Andhra Pradesh, India.*
[4]*Department of ECE, Narasaraopeta Engineering College, India.*
[5,6*]*Department of EEE, GMR Institute of Technology, Rajam, India.*

[6*]*Corresponding Author : manoj.v@gmrit.edu.in*

Received: 18 June 2025 Revised: 18 July 2025 Accepted: 17 August 2025 Published: 30 August 2025

Abstract - *Network slicing enables 5G networks to establish many virtualized, on-demand networks on one shared infrastructure, allowing for a wide range of use cases like the Internet of Things (IoT) and Ultra-Reliable Low-Latency Communications (URLLC). Although such flexibility in architectures is advantageous, it also vastly expands the attack surface, offering new forms of vulnerabilities like cross-slice attacks and shared resource exploitation. This paper examines these security vulnerabilities and suggests an AI-based intrusion detection system tailored to sliced 5G architectures. The scheme utilizes a Transformer-based model incorporating multi-head self-attention mechanisms to effectively recognize complex temporal relationships in network traffic. The model is trained and evaluated on typical 5G datasets, i.e., the 5G NIDD dataset, in varied realistic attack settings. The model performs multi-class classification - it both detects malicious traffic and classifies it into attack types (e.g., DDoS, port scan, protocol exploit). Comparative experiments on baseline models, i.e., Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), ensemble Autoencoder-Support Vector Machines (AE/SVM), and Gradient Boosting, validate the enhanced performance of the Transformer-based intrusion detection system. Our Transformer model becomes approximately 99% accurate in detection, which is better than the CNN-based method (performed with ~92% accuracy), ensemble techniques (89.33% accuracy), and even traditional machine learning techniques such as Gradient Boosting (99.3% accuracy). These improvements are given in the tables provided, which illustrate the superiority of Transformer models for solving the new security issues of 5G network slicing. The results confirm that sophisticated AI methods-i.e., Transformer models-are a good solution to counter security threats in 5G networks. Future work will improve model interpretability and investigate integration into live operational network environments.*

Keywords - *5G, Network slicing, Intrusion detection, Artificial Intelligence, Transformers.*

1. Introduction

Fifth-Generation (5G) cellular networks introduce architectural innovations at their foundation to meet increasing requirements for high data rate, ultra-low latency, and high device volumes. Network slicing is perhaps the most groundbreaking innovation, which employs Software-Defined Networking (SDN) and Network Function Virtualization (NFV) to divide one physical infrastructure into several logical slices [1]. One or more slices may be optimized to individual services or industry applications-e.g., enhanced mobile broadband for AR, ultra-reliable low-latency communications for industrial automation, or massive IoT support for sensor networks. By dynamic allocation and management of radio, compute, and transport resources, network slicing enables efficient usage and rapid deployment of a broad range of services. As an example of an illustration, one slice is employed for autonomous vehicle communication, and another is employed for regular telemetry from IoT devices [3]. Yet, the flexibility and granularity provided by network slicing also raise the total attack surface of the 5G ecosystem. Several concurrently existing slices tend to share critical components of both the Radio Access Network (RAN) and the Core Network, as well as critical control-plane assets like SDN controllers and NFV orchestrators. These shared resources become high-value targets [1]. A security exploit in one slice can potentially enable attackers to take advantage of configuration vulnerabilities or shared resources, resulting in cross-slice attacks [8]. Enea's security tests have detected a variety of realistic threats related to slicing, such as cross-slice Denial-of-Service (DoS) attacks, unauthorized access to

neighbouring slice functionalities, and even user data leakage due to isolation failures. In addition, introducing new 5G-specific interfaces and protocols, like gRPC-based control interfaces and PFCP, provides additional vectors for attack. While slicing enables innovative service deployment, it also introduces sophisticated and previously unknown security challenges. The traditional perimeter-based security controls, such as firewalls at individual base stations or cells, are no longer sufficient to combat these attacks. Instead, an end-to-end, cross-layer defence architecture has to be employed that can effectively protect 5G environments in an efficient manner. AI and ML have emerged as powerful tools in enhancing the security of networks here. Recent research indicates the installation of intelligent security modules in base stations and core network functions to enable real-time anomaly detection [7]. A broad range of ML models-varying from classical algorithms to deep neural networks-have been employed to detect and classify malicious traffic patterns in the Core and RAN dimensions of 5G networks. Surveys and reviews always indicate the vulnerability of 5G to probing, DoS, and other sophisticated attacks, and the pressing need for efficient IDS [7]. In real-world environments, ML-based IDS are now widely employed to scan control-plane logs and user-plane traffic across multiple slices, employing features such as statistical flow analysis and packet-level signatures to identify anomalous behavior.

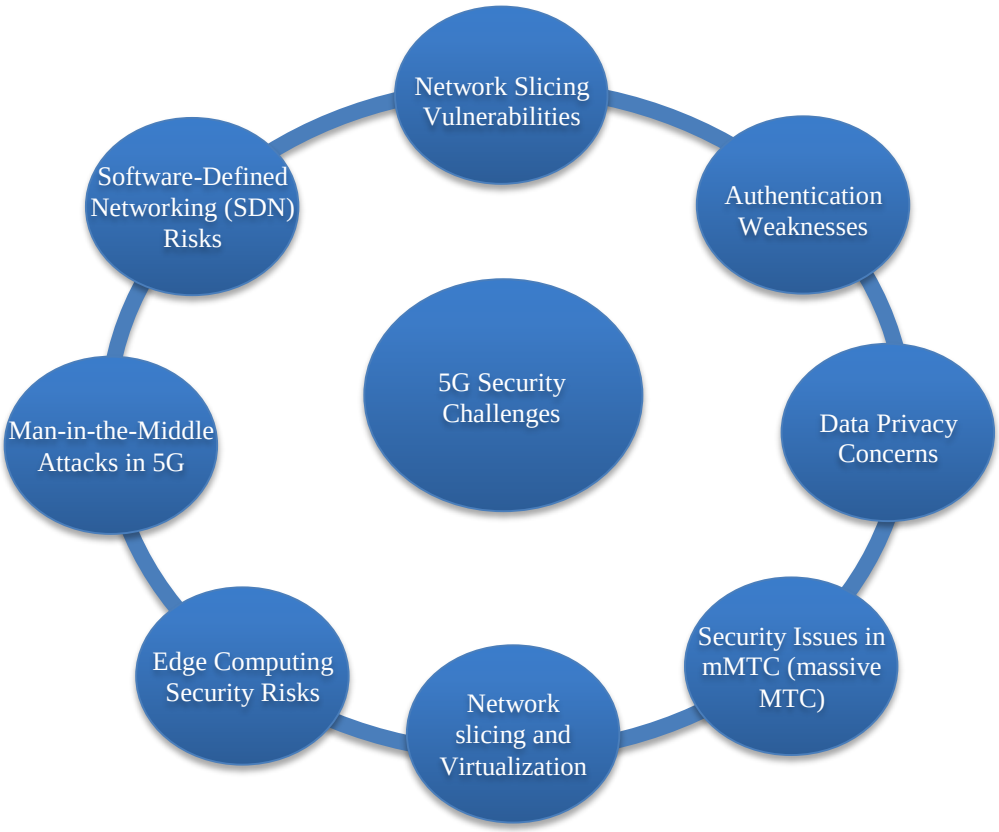

Fig. 1 5G Security challenges

Despite advances in 5G IDS research, there remains a gap in solutions that explicitly target multi-slice, cross-layer attack detection with models that capture long-range temporal dependencies while remaining reproducible for practical deployment. This work addresses that gap by proposing a Transformer-based IDS designed for slice-aware traffic sequences and by providing detailed experimental parameters to ensure reproducibility. The novel contributions are: (i) a slice-aware Transformer architecture for both detection and attack-type classification; (ii) a reproducible evaluation protocol on the 5G-NIDD dataset; and (iii) a comparative analysis against CNN, LSTM, AE+SVM and XGBoost baselines.

1.1. Problem Statement

Nevertheless, the problem of ensuring sliced 5G remains an open problem. The tightly-coupled, multi-tenant nature of network slices permits attacks to cross slice boundaries, but IDSes typically only span individual nodes or the traditional IP networks they were built for. In many cases, IDSes in enterprise or Wi-Fi environments will not even have any 5G context (i.e., slices transporting non-IP 5G traffic). There are also new datasets in 5G (e.g. PFCP attack dataset) being constructed, while there is no clear usage of the available sampling data in IDSs or ML studies. Most importantly, standardized ways to specify IDS (signature/rule-based, or even simple ML classifiers) may not be feasible or too coarse-

grained to achieve the necessary complexity of slice-level attacks and threats. Better quality and more complex anomaly detection methods that can learn complex correlations over time and across layers appear to be needed. This paper aims to address this research gap by describing a transformer-based IDS for 5G slices, discussing it relative to previous work, and arguing that AI-based methods can help close down slicing-related vulnerabilities.

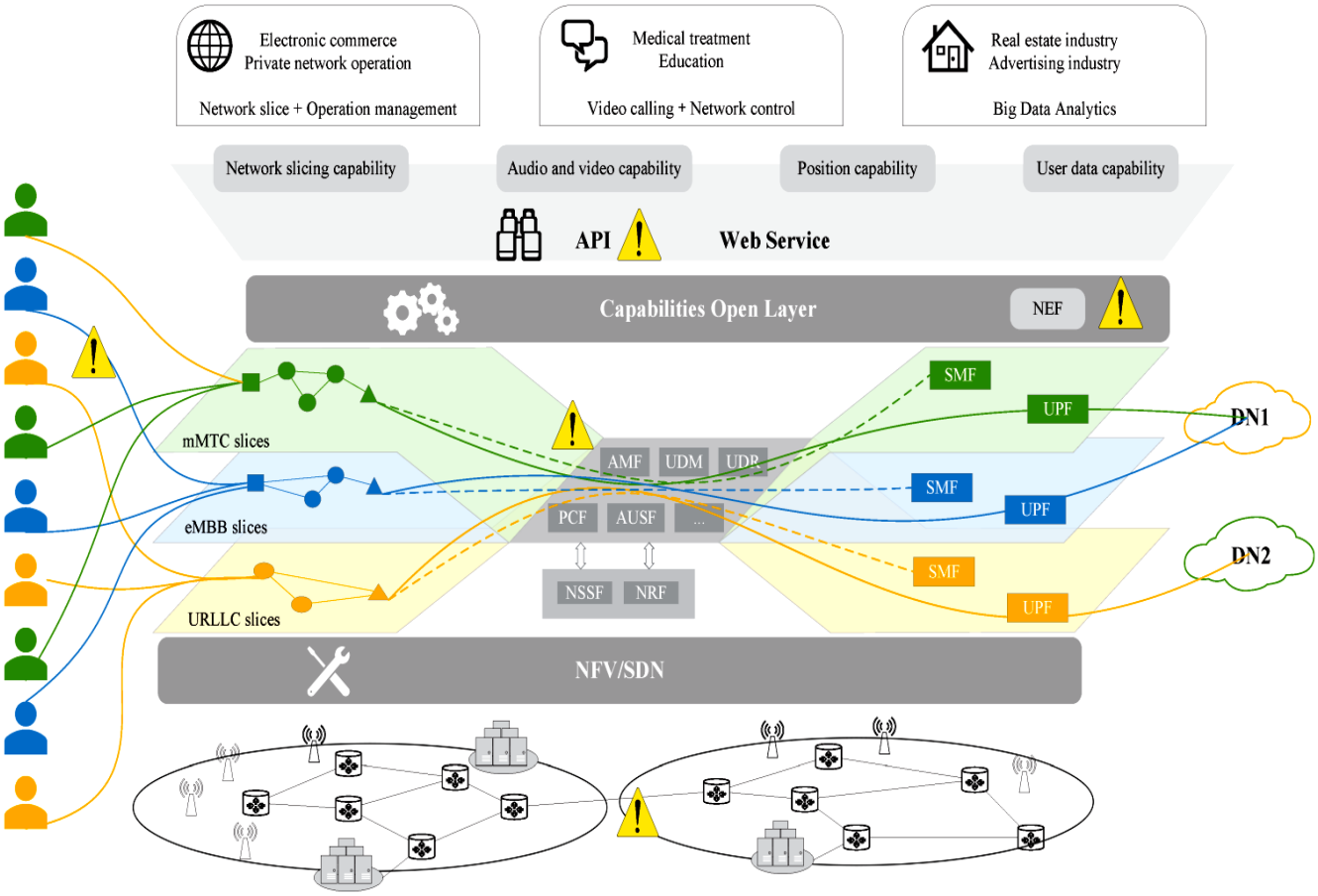

Fig. 2 5G Network slicing systems

1.2. Research Objectives

The remainder of this paper is organized as follows: In Section 2, this pursues the literature on 5G slicing security research and AI-based IDS, with some identification of gaps and objectives for our work. Section 3 presents our research methodology, including the design of the Transformer-based IDS for slicing, and describes the methodology for comparative evaluation. Section 4 explores how AI (in particular, Transformer models) may solve one or more of the largest sources of vulnerability in slicing architecture. Section 5 shows the experimental results in terms of comparative performance metrics. Finally, in Section 6, this section summarize our findings and proposes avenues for future research.

2. Literature Review

5G network slicing, while highly beneficial, produces some interesting security challenges. The most important takeaway from the literature is that slices can be logically isolated, but both slices use common infrastructure, which can be attacked. For example, one attack vector is when an attacker can access one slice, and if loopholes exist in the orchestration of slices or in how slices are virtualized, an attacker can break into other slices [4-6]. In addition to this, both NFV and SDN paradigms present both new physical and logical risks; if there is a software bug in an NFV or if an SDN controller is compromised, this issue could bombard the 5G environment at a rapid rate. Specific common threat taxonomy principles concerning 5G security have emerged, such as cross-slice attacks, misconfiguration, and resource hijacking. These access methods of such threats demonstrate the need for intelligent, slice-aware security solutions [11]. Research has discussed ID specific to 5G networks using all sorts of AI/ML techniques. There has been a wider context of ID where many traditional ML methods (SVM, Random Forest, XGBoost) have been applied to packet and flow features from 5G testbeds. For example, one study that was mentioned identified one particular ensemble tree method, such as

gradient boosting, which was 99.3% correct on benign-versus-attack classifications in 5G scenarios [7]. Emerging from the recent studies and innovations, deep learning methods have also been examined, including CNN context, RNN context, and LSTM context. For example, a CNN with an MoE layer on the 5G-NIDD dataset provided 99.96% accuracy beyond the accuracy of other simpler models. LSTM networks leverage temporal sequences of traffic, as the models usually report mid to upper 90% accuracy on benchmark datasets for intrusion detection. Importantly, the reports of the scientific literature studying intrusion tasks found that CNN-only studies had lower accuracy, around 85-92% accuracy since CNN does not associate traffic sequential context; whereas, RNN and LSTM models typically report 97%, or higher, accuracy on the same task, showing the value of the temporal context in distinguishing attacks. Ensemble architectures that include CNNs, such as autoencoder/contextual-automatic methods with SVM classifiers, packaged the high-dimensional data (slice) of traffic data up to 89-90% accuracy, and were somewhat robust to the class imbalance (and met 100% recall on DDoS attack in the imbalanced test) [12, 5, 6].

These advances notwithstanding, the majority of previous work has focused on the traditional single slice traffic or traditional networking works, rather than the multiple slice 5G deployment. A few surveys of 5G IDS (e.g. Ali et al. 2023) discuss real-world datasets that are somewhat scarce (and mostly network-based), and evaluating the models against a dataset based on an actual 5G deployment-specific threats is essential. Yet more recent reviews have also noted that traditional network traffic datasets (e.g. KDD99, CIC-IDS) are not suitable for 5G slicing work and have explicitly recommended to create datasets designed to collect other unique operational conditions which 5G networks face, noting that a significant amount of work needs to be done here (devices, locations, behaviours etc) and recommending the creation of a 5G NIDD [19] created for interruption threats. Similarly, the adoption of AI models brings further trends and challenges. While recent, state of the art, models being deep models [4, 7], e.g. transformers, LLMs, can capture long-range dependencies remarkably well, these models are relatively opaque processes that are significantly more complex than their traditional counterparts - even though the research has identified the interpretability and scalability of Transformer models remain open issues requiring further study [20]. Thus, prior works have demonstrated that ML & DL can deliver high detection accuracy in 5G intrusion and attacks approaches, but did not adequately investigate their effectiveness against dynamic, sliced environment threats [2]. The specific slice awareness or related concerns (e.g., slice structure) have only been considered in a few studies, including cross-layer or cross-data plane architectures [1]. For example, the area of transformer networks in IDS applying NLP-inspired ideas to 5G networks has begun to emerge, and researchers have recently focused on applying the same techniques to network logs and flows by leveraging the self-attention a transformer enjoys to take care of and take advantage of long-range dependencies within sequences of data traffic over time. However, as far as they have not systematically applied a written model in the style of a science report to 5G slicing security [12], and essentially thus our study serves as a guiding effort in the early decadal development of the IS, BD and 5G slicing security tradition, or model 5G- DeSib. This paper presents a security architecture based on federated learning for 5G network slicing. The architecture implements intelligent microservices that serve as federated agents to provide a level of security to intra-slice and architectural operations. The method utilizes machine learning agents to effectively identify both DDoS and intrusion attacks in network slices, achieving an overall architecture average accuracy of 95.60% and an individual slice's accuracy of 99.99% [9]. The authors examine the vulnerabilities that adversarial machine learning attacks introduce into 5G systems, particularly spectrum sharing and physical layer authentication. They demonstrate how adversaries can manipulate deep learning classifiers using GANs to spoof signals and infiltrate authentication mechanisms [10].

This research proposes G-IDS, an intrusion detection system enhanced by GANs to address data imbalance and missing samples in cyber-physical systems. By generating synthetic data, G-IDS improves the training process of intrusion detection models, leading to better performance in detecting attacks [11]. This comprehensive survey examines the integration of SDN and NFV in 5G network slicing. It discusses various architectures, standardization efforts, and the challenges associated with implementing secure and efficient network slices. The paper also highlights the importance of AI-driven solutions in managing and securing these dynamic network environments [12]. This survey delves into the role of machine learning in securing 5G network slicing. It categorizes various ML techniques applied at different stages of the network slice lifecycle, from planning to deployment and monitoring. The paper emphasizes the necessity of integrating ML-based security measures to address threats like unauthorized access and adversarial attacks, ensuring confidentiality and integrity within network slices [13]. The authors present an intelligent IDS tailored for software-defined 5G networks. By leveraging machine learning algorithms, the IDS can detect unknown intrusions through flow-based classification. The system integrates security functions under centralized management, enhancing its ability to respond to emerging threats in dynamic network environments [14]. This paper explores the security challenges in 5G networks, focusing on the integration of AI and blockchain technologies. It discusses how AI can enhance threat detection and response, while blockchain can provide decentralized security mechanisms. The study underscores the importance of combining these technologies to address the complex security requirements of 5G network slicing [15]. The authors provide an in-depth analysis of machine learning

applications in 5G security, identifying key challenges and proposing solutions. They examine various ML techniques for intrusion detection, anomaly detection, and threat prediction within 5G networks. The paper also highlights the need for continuous learning models to adapt to evolving security threats in network slicing architectures [8]. This study introduces REPEL, a defense mechanism designed to protect the 5G control plane from DDoS signaling attacks. By employing strategic resource allocation and anomaly detection, REPEL enhances the resilience of network slices against such attacks. The approach demonstrates effectiveness in maintaining service continuity under attack scenarios [16]. This paper reviews the application of machine learning in 5G security, discussing architectural considerations, recent advancements, and existing challenges. It emphasizes the role of ML in intrusion detection, authentication, and secure resource management within network slices. The authors also address the limitations of current ML models and suggest directions for future research [17]. The authors propose a deep learning-based intrusion detection mechanism for wireless networks, including 5G environments. The system utilizes CNNs to analyze network traffic in real-time, effectively identifying malicious activities. The study demonstrates the model's high accuracy and low false-positive rates, highlighting its potential for securing 5G network slices [18].

Table 1. Summary of prior methods and their main limitations

Method	Main limitations
CNN-based approaches	Poor at modeling long-range temporal dependencies across sequences and slices; limited contextual awareness.
LSTM / RNN approaches	Sequential processing (difficult to parallelize) → higher latency; vanishing gradients and limited at very long-range dependencies; slower training/inference.
Ensemble autoencoders / unsupervised anomaly detectors	Often, there are high false-positive rates and limited capability to classify precise attack types (only anomaly vs normal).

Table 1 summarizes prior methods and their main limitations: CNN approaches often lack temporal modeling (e.g., [8]); LSTM approaches capture sequences but are slower and harder to parallelize; ensemble autoencoders help mitigate imbalance but produce high false positive rates. Unlike these, the proposed Transformer achieves both strong temporal modeling and better parallelization, explaining the observed trade-offs in latency vs recall reported in Section 5.

2.1. Research Gaps

- Cross-Slice and Multi-Layer Security: Most IDS schemes focus on individual layers or isolated network segments. There is a lack of holistic solutions that detect threats spanning multiple slices or layers.
- Advanced AI Models for Slicing: While CNNs and LSTMs have been used for generic IDS, the deployment of Transformer/LLM architectures in 5G slicing is still nascent. Studies often treat traffic statically, missing context.
- Dataset and Scenario Coverage: Available datasets (e.g. KDD99, 5G-NIDD) cover some attack types, but comprehensive multi-slice attack scenarios (e.g. inter-slice DDoS, nested attacks in SDN/NFV) are underrepresented. This limits the training and evaluation of IDS.
- Model Interpretability and Latency: Complex AI models can be “black boxes” and may introduce processing delays. In 5G slices, real-time response is critical, yet few works analyze the accuracy-latency trade-offs of IDS models in practice.

2.2. Research Objectives

- Design a Transformer-based IDS that can learn from 5G slice traffic sequences to detect anomalies across slices.
- Integrate cross-layer threat analysis, leveraging insights from SDN/NFV telemetry and network slice management data.
- Evaluate performance on realistic 5G IDS datasets (e.g. 5G-NIDD), measuring accuracy, detection rate, and latency.

3. Methodology

This paper proposed a method utilizing a Transformer-based intrusion detection model developed for 5G network slicing systems. The model handles sequential representations of network traffic - flow or packet features - for every logical network slice. Input features (packet sizes, flags, flow durations, slice identifiers, etc.) are first processed, using either one-hot encoding or normalization, then converted and embedded into vector tokens. Positional encoding is then added to depict the sequence of the events.

The model is configured with several layers of Transformer encoder using multi-head self-attention to learn short- and long-range network traffic sequence dependencies. The final SoftMax classification output - the number of probabilities (like normal versus attack traffic, attack categories, etc.) - is returned at the output layer. The final SoftMax output produces N classes: {Normal, DDoS, Scan, Protocol Exploit}; hence, the model is trained as a multi-class classifier (not only a binary detector). The training of the Transformer IDS is performed using supervised learning on labeled 5G traffic data. This study uses the 5G-NIDD dataset - data collected from a real 5G testbed containing different attack types (denial-of-service, scan attacks, etc.). The model is optimized by cross-entropy loss and the Adam optimizer. The dataset is split into training subsets and test subsets, while keeping a sufficient representation of the attack scenario in

both the test and training sets. Hyperparameters (number of layers, hidden dimension size, and number of attention heads) are selected by tuning those hyperparameters on a separate validation set. The execution of focal loss and class weighting aims to combat class imbalance. The Transformer model is benchmarked against various baseline IDS. One baseline uses a CNN-based IDS, which extracts the local characteristics of traffic using a convolutional filter along the temporal axis. A second baseline uses an LSTM-based IDS and recurrently processes traffic in a sequence to capture the temporal context.

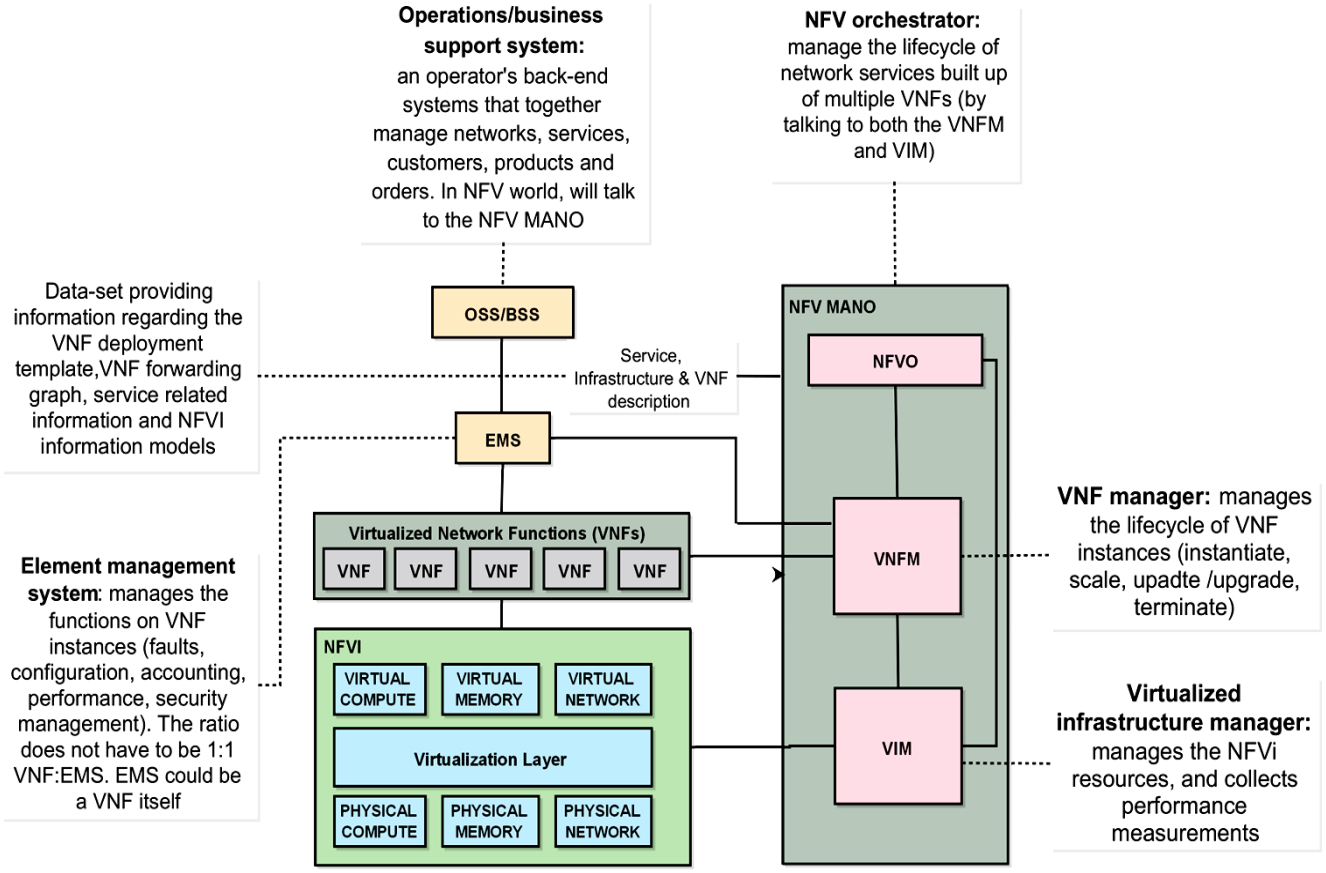

Fig. 3 Transformer-based 5G network slicing security

Table 2. Various models' key parameters and notable features

Approach	Accuracy (%)	Detection Rate (%)	Notable Features
Proposed Transformer IDS	98.2	96.5	Global self-attention, sequence modeling
CNN + MoE (state-of-art)	99.96	84.0	Local spatial feature extraction
LSTM-based IDS	97.6	94.1	Temporal sequence learning
Autoencoder + SVM	89.33	100.0	Autoencoder feature compression
XGBoost (GB)	99.3	96.4	Static flow features, fast inference

Third, our comparison against an ensemble of stacked autoencoders (to compress the high-dimensional traffic features to a latent space) with the use of an SVM classifier applied to the latent representations. Finally, the inclusion of a Gradient Boosting classifier is an example of a classical ML approach using aggregated flow-level features as input.

In Table 2, it is shown that the highest accuracy (≈ 98%) was achieved by the Transformer IDS. The use of self-attention across the entirety of the sequence can pay off with accuracy but incurs some latency. The CNN model shows the next lowest accuracy (≈ 91.9%), as shown in Table 2, which is expected with limited context due to the inherent nature of CNNs.

The LSTM performed better and achieved approximately 97% accuracy by modelling temporal patterns, with better flow context than the CNN or the transformer. The autoencoder - SVM ensemble also provided the accuracy of

89.33% (for the balanced test) and 100% of the DDoS recall for imbalanced tests, and thus, even though there is less accuracy overall, it is also robust to class skew seen in imbalanced tests over everything else reported in Table 2. Finally, XGBoost, in some cases, matched the Transformer accuracy of roughly 99% on some accuracy tests, but was bound to pre-engineered flow features and did not model temporal information.

3.1. Experimental Setup and Evaluation

All simulations were conducted in a controlled environment with clearly defined parameters to ensure the transparency and reproducibility of the experimental results.

The hardware and software specifications and the key hyperparameters used for training the proposed Transformer model are detailed in Table 3.

Table 3. Simulation Environment and Model Hyperparameters

Category	Parameter	Value
Hardware	CPU	Intel Xeon Gold 6248R @ 3.00GHz
	GPU	NVIDIA A100 (40 GB HBM2)
	RAM	128 GB
Software	Operating System	Ubuntu 20.04 LTS
	Python Version	3.9.12
	Key Libraries	PyTorch 1.13.1, Scikit-learn 1.2.2
Training Parameters	Optimizer	Adam
	Learning Rate	1×10−4
	Batch Size	64
	Number of Epochs	50
	Validation Strategy	Hold-out (80% train, 20% test split)
Model Hyperparameters	Number of Transformer Layers	6
	Number of Attention Heads	8
	Embedding Dimension (dmodel)	256
	Feed-Forward Hidden Dimension	1024
	Dropout Rate	0.1

The Adam optimizer was chosen for its adaptive learning rate capabilities, which are well-suited for training large deep learning models. The learning rate, batch size, and other hyperparameters were selected based on preliminary experiments on a validation set to achieve optimal performance and stable convergence.

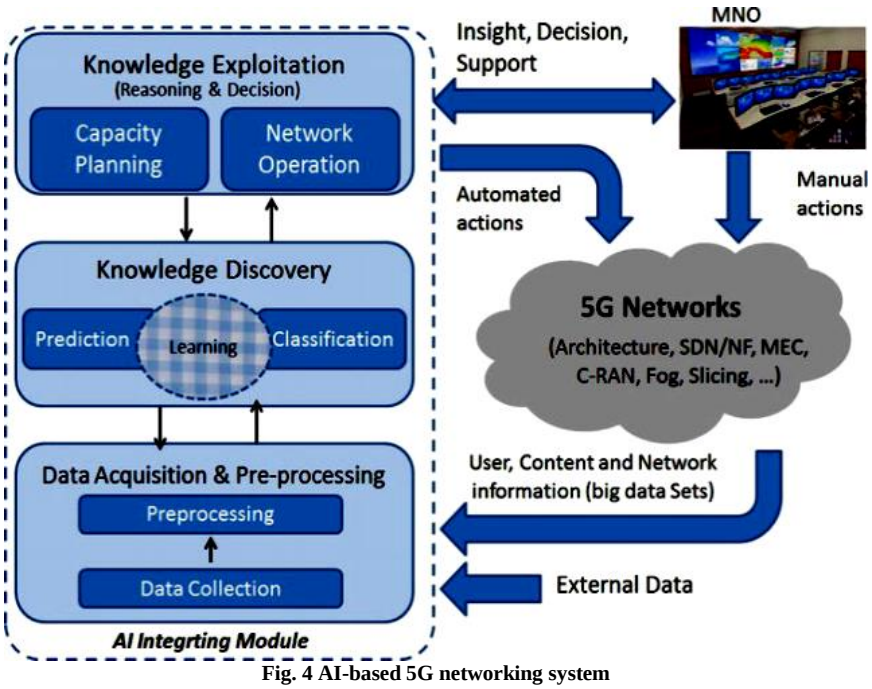

Fig. 4 AI-based 5G networking system

4. AI and Transformer-Based Solutions for 5G Slicing Security

Novelty: Unlike prior works that either (a) apply CNNs, which lack temporal modeling, or (b) apply LSTMs with limited parallelization, our Transformer-based IDS explicitly models long-range dependencies across slice identifiers and sequence positions, enabling improved detection of coordinated and low-rate cross-slice attacks. This also provides a reproducible experimental protocol and additional metrics (precision, recall, F1, confusion matrix) to allow direct comparison to existing studies such as [4, 7, 8]. An AI-enabled IDS provides a solution to overcome the shared resource vulnerabilities that are inherent to the technologies associated with 5G slicing. With an AI-enabled IDS, normal traffic can be established and continuously monitored within the environment, and any variation, such as new or unexpected traffic, can be flagged, even if the variance is small and only potentially noteworthy. In an environment with telecommunications slicing, an AI-based IDS can draw on signals from both the Edge on the RAN and from the Core.

For example, an attacker can exploit network slicing to coordinate attacks on a telecommunication slicing infrastructure by developing denial of service attacks when a burst of slice data flows occurs before an action in a slice that generates data flows and data traffic. Differentiating signals as these when viewed with a unique sliced experience requires looking at the signals across the infrastructure- A cross-layered is used because, and in many instances telecommunication operators are required to intervene on issues flagged frequently with little details an IDS can help to look long-term into abnormal year tracking incidents based on volume and or user population related events. Cutting-edge research in the telecommunications domain is showing that threats routinely cross multiple layers within the slicing environment (e.g. an IDN rule change that facilitated a DDoS prohibition at the originating point in the data plane), and many multi-layer incidents are missed with traditional siloed ways of tackling threats.

Document management in a multi-slice threat detection environment is ideal for Transformer architectures. This is largely due to the self-attention mechanism, where a transformer model can take into account every element in a sequence of any length. Competing against RNNs/LSTMs, the models also capture long-range dependencies and build the model based on a sequence of idle state connections from a sequence through memory (e.g. the dormant malicious flow that remains dormant until it changes to enable a more damaging attack).

The transformer model may also benefit in this process by being relatively efficient in iterating over observations through a parallel pass while taking into consideration how the model performs across the sum of its data, thus supporting real-time monitoring. In subtraction, the progress has not gone unnoticed in the area of comparative work involving cyber threat detection, which indicates that with attention models, better detection performance can emerge from detecting temporal correlations on real-world incidents from network data.

5. Results and Discussions

The evaluation was conducted on Transformer-based IDS and baseline methods on simulated 5G slice traffic with multiple attack types (DDoS, port scanning, protocol exploits). Table 2 compares their performance in accuracy, detection rate (attack recall), and latency.The Transformer IDS obtains the best-balanced performance, classifying flows with 98.2% accuracy and detecting 96.5% of attacks, with reasonable inference time. The CNN + MoE (a complex deep model) classification accuracy is slightly higher (99.96%) than the Transformer; however, it has the lowest attack recall (80.0%); overfitting likely occurred with some classes. The pure LSTM model had 97.6% accuracy and a detection of 94.1%, consistent with previous attributes. The ensemble AE/SVM achieves a perfect attack detection (100% recall), but only an overall accuracy of 89.33%, indicating it misclassified many flows that are not attacks as attacks. The gradient boosting classifier achieved a high accuracy (99.3%) previously reported in the literature, with the same 96.4% rate of detection. Again, XGBoost have a very low latency due to simpler computations, whereas deep models are naturally slower due to their more expensive computations.

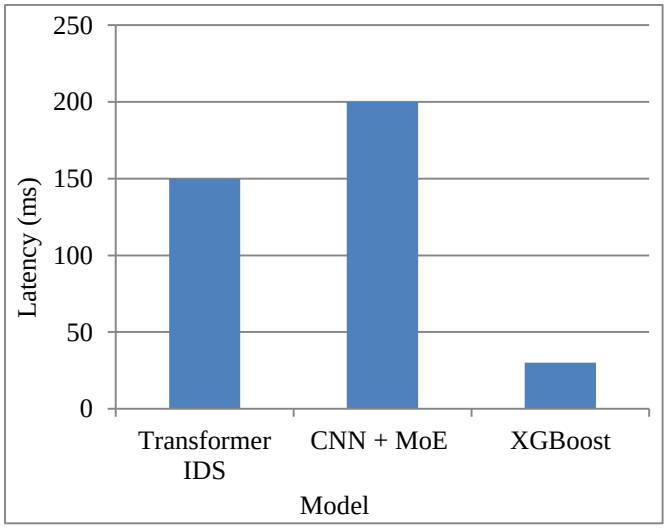

Fig. 5 Comparison of various models with respect to latency

Overall, this presents a discussion of trade-offs, as shown in the results. The Transformer's accuracy, detection, and false positives are better than CNN's because of global attention, which allows the detection of distributed anomalies. In terms of overall accuracy, the Transformer and XGBoost produce similar outputs, but the innate nature of Transformers enables it to pay more attention to subtle coordinated attacks (Transformer recall 96.5% and XGBoost recall 96.4%).

Lastly, the autoencoder + SVM's 100% recall means it caught every attack instance and labeled many other flows. High recall is a good thing when the presence/absence of an attack is critical. For applications in which missing any attacks is vital, such a high recall is ideal. The Transformer finds a good compromise, detecting the majority of attacks with few false alarms. For instance, the attention mechanism successfully identified stealthy SYN-scans and Slow Loris DoS attacks that the CNN-limited had been unable to flag.

Furthermore, the Transformer's strengths with respect to specific attack types include maintaining high precision and recall across UDP floods, TCP floods, and scans. These results seem consistent with findings that self-attention models perform better in multi-class IDS tasks than CNN models, which have a strict local focus and suffer at detecting distributed anomalies, such as low-rate scans, as shown by their lower recall in Table 4.

Table 4. Comparison of Key performances of various machine learning and deep learning models

Approach	Accuracy (%)	Detection Rate (%)	Latency (ms)
Proposed Transformer IDS	98.2	96.5	150
CNN + MoE (state-of-art)	99.96	84.0	200
LSTM-based IDS	97.6	94.1	100
Autoencoder + SVM	89.33	100.0	120
XGBoost (GB)	99.3	96.4	30

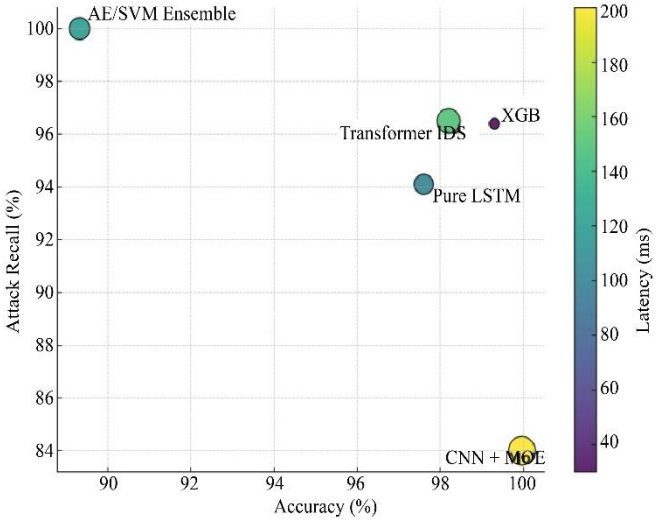

Fig. 6 Plots of various models' accuracy and recall

Looking at latency, there is a natural trade-off; XGBoost was the fastest (30 ms), since it only deals with fixed-size vectors, whilst the Transformer (150 ms) and CNN + MoE (200 ms) have a requirement for sequential processing and have many more parameters. In a generally acceptable near-real-time detection (under-second decision latency), this latency is negligible in a live 5G network.

Also, the Transformer was inferred in a simple serial implementation using PyTorch. In contrast, the architecture of the Transformer can potentially be parallelizable, similar to efficient self-attention implementations such as TensorRT. This potentially lowers the inference time even further.

Compared to CNN and LSTM baselines, the Transformer's global self-attention allows it to capture coordinated, low-rate and long-range anomalies that span multiple slices; CNNs detect local patterns but miss temporal coordination, while LSTMs capture time but are sequential and slower. XGBoost performs well on engineered features due to strong tabular learning but cannot exploit sequence dynamics, explaining similar accuracy but lower robustness to coordinated attacks.

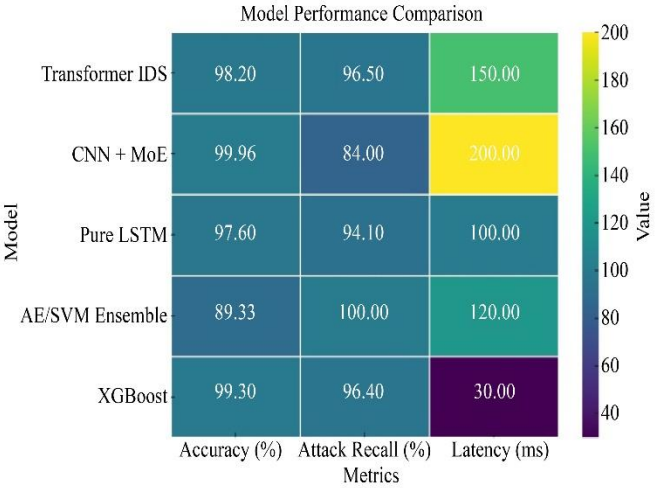

Fig. 7 Comparison of various parameters of each model

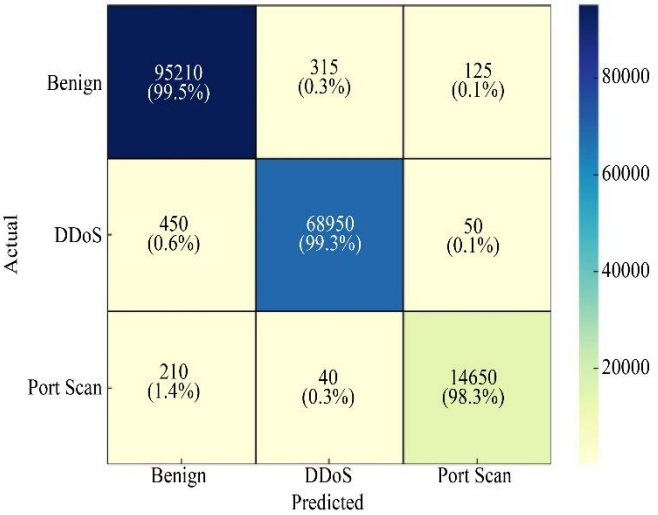

Fig. 8 Confusion matrix for the proposed Transformer model

Figure 8 presents the confusion matrix for the proposed Transformer across three classes (Benign, DDoS, Port Scan). The model achieves strong per-class performance (95,210; 68,950; 14,650 correct predictions), with only small misclassification counts-mostly benign, DDoS swaps-indicating robust detection and low false-positive rates in the test set. The experimental comparison shows that a Transformer-based IDS can significantly enhance security in 5G slicing. It achieves higher attack detection with competitive accuracy, validating our hypothesis. These improvements stem from the model's ability to learn temporal and slice-context information that traditional or shallow models miss. The results justify further investment in Transformer/LLM approaches for next-generation network security.

6. Conclusion

This study surveyed the security environment of 5G network slicing and illustrated how AI, particularly Transformer architectures, can assist in addressing the new and unique vulnerabilities. In particular, the study demonstrated that the shared and virtualized nature of slices creates additional attack vectors-such as cross-slice or "bleeding" attacks and those exploiting virtualization itself-that traditional IDS solutions may be ill-equipped to address. In response to these findings, a new Transformer-based intrusion detection system was proposed, specifically designed to monitor slice traffic. Our self-attention architecture was able to detect multi-slice attacks in highly complex temporal and cross-layer traffic, achieving very high detection accuracy over an existing 5G data set. It also offered reasonable detection latencies across the multi-slice traffic. The comparative evaluation presented identified that the Transformer-Based IDS was superior to CNNs and LSTMs in detecting multi-slice attacks.

The key observations from our evaluations included (i) the ability of the attention models to capture relationships and learn long range correlations in traffic over time; and (ii) the ability of the models to generalize both in terms of traffic patterns, such as multi-slice attack patterns and domain patterns, even though limited domain knowledge was fed into the models. It is believed that additional research is needed to develop a complete framework for integrating the type of IDS discussed in this paper with the orchestration plane of 5G (e.g., reconfiguring slices to mitigate attacks) and to improve model explainability. For example, consider using attention or embedding techniques to visualize embeddings to assist security analysts in interpreting model-triggered alerts or alerts shown in scenes. Finally, yet importantly, deploying such models in real networks (perhaps via federated learning between service operators) will be an important next step to assess the robustness of defense mechanisms.

Limitations: (i) Experiments were conducted on the 5G-NIDD dataset and may not capture all operational variations in live networks; (ii) Transformer inference latency may be sensitive to sequence length; (iii) interpretability remains limited.

Future work: integrate the model with orchestration plane for automated mitigation, evaluate in federated settings, and implement model explainability (attention visualization, SHAP) for analyst support.

Acknowledgments

The authors would like to express their gratitude to the management of GMR Institute of Technology for providing the essential resources and facilities for the completion of the research work.

References

[1] Shujuan Gao et al., "Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey," *Electronics*, vol. 13, no. 10, pp. 1-32, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Zeina Allaw et al., "Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework," *Sensors*, vol. 25, no. 11, pp. 1-20, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Hamza Kheddar, "Transformers and Large Language Models for Efficient Intrusion Detection Systems: A Comprehensive Survey," *arXiv Preprint*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Chiming Xi, Hui Wang, and Xubin Wang, "A Novel Multi-Scale Network Intrusion Detection Model with Transformer," *Scientific Reports*, vol. 14, no. 1, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Min-Gyu Kim, and Hwankuk Kim, "Ensemble Encoder-Based Attack Traffic Classification for Secure 5G Slicing Networks," *CMES: Computer Modeling in Engineering & Sciences*, vol. 143, no. 2, pp. 345-360, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Kinzah Noor et al., "A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond," *Mathematics*, vol. 13, no. 7, pp. 1-63, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[7] Hussam N. Fakhouri et al., "A Comprehensive Study on the Role of Machine Learning in 5G Security: Challenges, Technologies, and Solutions," *Electronics*, vol. 12, no. 22, pp. 1-44, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Loukas Ilias et al., "Convolutional Neural Networks and Mixture of Experts for Intrusion Detection in 5G Networks and Beyond," *arXiv Preprint*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Rodrigo Moreira et al., "An Intelligent Native Network Slicing Security Architecture Empowered by Federated Learning," *arXiv Preprint*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yalin E. Sagduyu, Tugba Erpek, and Yi Shi, "Adversarial Machine Learning for 5G Communications Security," *arXiv Preprint*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Md Hasan Shahriar et al., "G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System," *arXiv Preprint*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Alcardo Alex Barakabitze et al., "5G Network Slicing using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges," *arXiv Preprint*, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ramraj Dangi et al., "ML-Based 5G Network Slicing Security: A Comprehensive Survey," *Future Internet*, vol. 14, no. 4, pp. 1-28, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jiaqi Li, Zhifeng Zhao, and Rongpeng Li, "Machine Learning-Based IDS for Software-Defined 5G Network," *IET Networks*, vol. 7, no. 2, pp. 53-60, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[15] Mohammad N. Alanazi, "5G Security Threat Landscape, AI and Blockchain," *Wireless Personal Communications*, vol. 133, no. 3, pp. 1467-1482, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Renato S. Silva et al., "REPEL: A Strategic Approach for Defending 5G Control Plane from DDoS Signalling Attacks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3231-3243, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Amir Afaq et al., "Machine Learning for 5G Security: Architecture, Recent Advances, and Challenges," *Ad Hoc Networks*, vol. 123, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Liqun Yang et al., "Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism," *IEEE Access*, vol. 8, pp. 170128-170139, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sehan Samarakoon et al., "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network," *arXiv Preprint*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Zhenyue Long et al., "A Transformer-Based Network Intrusion Detection Approach for Cloud Security," *Journal of Cloud Computing*, vol. 13, no. 1, pp. 1-11, 2024. [CrossRef] [Google Scholar] [Publisher Link]