

Advancing Predictive Security for Consumer Applications in Beyond 5G/6G Networks With Annotated Datasets

George Xylouris¹, *Member, IEEE*, Athina Vekraki, Maria Christopoulou², *Member, IEEE*, Michail Alexandros Kourtis³, Evangelos K. Markakis⁴, *Member, IEEE*, and Panagiotis Trakadas⁵

Abstract—The evolution of Beyond 5G (B5G) and 6G networks introduces new opportunities for consumer-centric applications, requiring robust predictive security measures to maintain reliability. A critical component in the B5G landscape is the Network Data Analytics Function (NWDAF), a Network Function (NF) of the 5G Core introduced by the 3rd Generation Partnership Project (3GPP) in Rel. 15, designed to provide data analytics capabilities to the cellular network. This study focuses on detecting Distributed Denial of Service (DDoS) attacks, leveraging a comprehensive dataset collected from a 5G testbed. We evaluate deep learning models—Convolutional Neural Networks (CNN), Long Short-Term Memory networks (LSTM), and Multi-Layer Perceptron (MLP)—and compare their performance with eXtreme Gradient Boosting (XGBoost), a machine learning technique based on gradient boosting, and Z-Score, a statistical method that quantifies how far a data point deviates from the mean. Results demonstrate that XGBoost achieves the highest F1-score of 0.97, precision of 0.96, and recall of 0.98, making it the preferred solution for identifying DDoS attacks from 5G network features, while also offering a computationally efficient solution for real-time applications. To improve interpretability, SHapley Additive exPlanations (SHAP) analysis identifies the network features influencing model decisions. The publicly available dataset used in our study supports further research in anomaly detection and provides valuable insights for future 6G applications, including immersive consumer experiences and autonomous services, while addressing emerging cyber threats.

Index Terms—3GPP, 5G, dataset, detection, DDoS attack, machine learning, NWDAF.

I. INTRODUCTION

THE FIFTH Generation (5G) of mobile networks marks a transformative milestone in cellular technology, designed to address the surging demands of an increasingly digital society. With its enhanced speed, consistent low-latency performance and expanded capacity, 5G supports a wide range of consumer-centric applications, from immersive augmented reality experiences to connected autonomous services. This evolution is underpinned by a shift toward a software-driven architecture that integrates virtualization, cloud-native technologies, and a Service-Based Architecture (SBA) to enable scalable and modular Network Functions (NFs).

Central to 5G's capability to deliver secure and seamless consumer experiences [1], [2] is the Network Data Analytics Function (NWDAF), introduced in the 3rd Generation Partnership Project (3GPP) Release 15. NWDAF facilitates data-driven and proactive network management through the collection and analysis of network data. From monitoring performance metrics and user behaviors to assessing real-time network conditions, the NWDAF serves as a critical enabler of optimized resource allocation, enhanced Quality of Service (QoS), and predictive anomaly detection.

The NWDAF interfaces with other 5G network functions within the SBA ecosystem through standardized protocols to provide actionable insights powered by advanced analytics and machine learning algorithms. NWDAF enables proactive network management by analyzing real-time data, optimizing resource allocation, and detecting anomalies. This capability of the 5G Core benefits predictive security in consumer applications, ensuring operational continuity and supporting adaptive configurations to maintain robust network performance and experience.

DDoS attacks present significant threats to 5G-powered consumer applications and smart city infrastructures. In Extended Reality (XR) applications, such as AR navigation, VR workspaces, and AR-assisted retail, these attacks can cause service disruptions, lag, and outages, affecting user experience and business operations. Similarly, smart cities rely on real-time 5G connectivity for traffic management, surveillance, public transport, and IoT-driven utilities. DDoS-induced failures in these systems can lead to traffic congestion, security vulnerabilities, and inefficiencies in energy and

Received 26 December 2024; revised 7 March 2025 and 4 April 2025; accepted 20 April 2025. Date of publication 5 May 2025; date of current version 14 August 2025. This work was supported by the Smart Networks and Services Joint Undertaking (SNS JU) through the EU Horizon Europe Programme PRIVATEER under Grant 101096110, through the Europe Programme HORSE-6G under Grant 101096342, and through iTrust6G under Grant 10113919. (*Corresponding author: George Xilouris.*)

George Xylouris is with the Institute of Informatics and Telecommunications, National Center for Scientific Research “Demokritos,” 15341 Athens, Greece, and also with the Department of Ports Management and Shipping, National and Kapodistrian University of Athens, 10679 Athens, Greece (e-mail: xilouris@iit.demokritos.gr).

Athina Vekraki and Michail Alexandros Kourtis are with the Department of Ports Management and Shipping, National Center for Scientific Research “Demokritos,” 15341 Athens, Greece (e-mail: avekraki@iit.demokritos.gr; akis.kourtis@iit.demokritos.gr).

Maria Christopoulou is with the Department of Ports Management and Shipping, National Center for Scientific Research “Demokritos,” 15341 Athens, Greece, and also with the Department of Informatics and Telecommunications, University of Peloponnese, 221 00 Tripoli, Greece (e-mail: maria.christopoulou@iit.demokritos.gr).

Evangelos K. Markakis is with the Electrical and Computer Engineering Department, Hellenic Mediterranean University, 71410 Heraklion, Greece (e-mail: emarkakis@hmu.gr).

Panagiotis Trakadas is with the Department of Port Management and Shipping, National and Kapodistrian University of Athens, 10679 Athens, Greece (e-mail: ptrakadas@pms.uoa.gr).

Digital Object Identifier 10.1109/TCE.2025.3567151

1558-4127 © 2025 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission.

See <https://www.ieee.org/publications/rights/index.html> for more information.

Authorized licensed use limited to: National Technical University of Athens (NTUA). Downloaded on March 16, 2026 at 05:39:59 UTC from IEEE Xplore. Restrictions apply.

waste management, highlighting the need for resilient defense mechanisms.

The key objectives of this paper are: (i) to evaluate AI/ML models for DDoS detection using annotated 5G testbed data, extending the work in [3], implementing the scenario outlined in [4]; (ii) to interpret model decisions using SHAP and assess the trade-off between accuracy and explainability; and (iii) to assess the feasibility of deploying such models in real-time in B5G/6G network scenarios.

These objectives formulate the research questions of this paper: (i) which models are most effective for DDoS detection on this dataset?, (ii) Can SHAP provide insights into the model decisions for anomaly detection?, and (iii) what are the considerations affecting the real-time deployment of these models in B5G/6G environments?

The subsequent sections of this paper focus on the exploration of Artificial Intelligence (AI)-driven anomaly detection in consumer applications within the context of Beyond 5G (B5G) and 6G networks. Section II reviews the State of the Art on advancements and challenges in AI-based security measures. Section III describes the frameworks, datasets, and experimental configurations employed in this study. Section IV presents the results and evaluates the performance of various machine learning and deep learning models, while the Discussion in Section V highlights key challenges in ensuring predictive security for consumer platforms. The work also explores how such advancements mitigate threats in real-world consumer platforms, from immersive AR/VR experiences to IoT-driven smart cities. Finally, the Conclusions summarize the findings and outline implications for future research.

II. STATE OF THE ART ON AI BASED ANOMALY DETECTION IN B5G NETWORKS

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as pivotal tools for addressing the evolving security challenges in Beyond 5G (B5G) and 6G networks [6]. These networks introduce complex applications and dynamic traffic patterns that demand sophisticated anomaly detection systems. Techniques such as Deep Learning (DL), Ensemble Learning (EL), and hybrid models are fundamental in enabling precise and scalable anomaly detection. Ensemble methods, such as Hybrid Adaboosting-Bagging Algorithms (HABBAs) [7], leverage diverse datasets, including NSL-KDD [8] and CIC-IDS2017 [9], to enhance detection accuracy across varied network behaviors. The integration of such datasets allows models to effectively distinguish between normal and malicious traffic, laying the groundwork for advanced feature selection strategies.

The optimization of feature selection is also significant for reducing unnecessary data while maintaining detection precision. Approaches, including Correlation-based Feature Selection with Random Forest (CFS-RF) [10] have shown promising results in minimizing false alarms and enhancing the detection of zero-day vulnerabilities—critical challenges in securing B5G systems. By focusing on relevant and high-impact features, these techniques improve anomaly detection efficiency [11], ensuring robust defenses against threats in

both user-facing [12] and management networks [7]. Such advancements highlight the importance of developing high-quality datasets protocols to support these models.

For anomaly detection systems to perform effectively, preprocessing steps such as data filtration [13], transformation [14], and normalization [15] enable models to generalize across real-world scenarios. Benchmark datasets, such as NSL-KDD, UNSW-NB15 [16], and CIC-IDS2017 provide valuable insights into traffic patterns and anomalies. Meanwhile, CICDDOS2019 [17], which focuses on Distributed Denial of Service (DDoS) attacks [18], is particularly relevant to address security threats prevalent in B5G environments. Such datasets will enable the optimization of AI/ML models to achieve high detection accuracy while minimizing false alarms, when trained in 5G-specific network features.

The Privateer Project [19] further exemplifies the critical role of domain-specific datasets in advancing anomaly detection for 5G and B5G networks. By capturing diverse DDoS attack vectors—such as SYN floods, ICMP floods, and DNS-based attacks—within a real-world 5G testbed, Privateer provides a comprehensive dataset incorporating control signaling metrics and radio access data [5]. The dataset adheres to 3GPP technical standards[20], bridging the gap between simulated and operational network environments. Importantly, they enable the evaluation and refinement of AI models using realistic traffic patterns and attack scenarios [3]. The project demonstrates how targeted metrics like uplink transmission rates and signal quality can enhance anomaly detection accuracy when integrated with advanced machine learning techniques such as Principal Component Analysis (PCA) and decision trees [21]. The availability of such datasets facilitates the development of explainable AI systems that provide actionable insights into security breaches while improving model interpretability.

There has been an increasing interest towards the detection of DDoS attacks against 5G networks. In [22], the authors leveraged 3GPP radio protocols (MAC, RLC, PDCP) to detect user plane DDoS attacks initiated by 5G UEs. The authors in [23], developed a near-Real Time (RT) RAN Intelligent Controller (RIC) to record measurements and identify the features of the physical and MAC layers used for detecting DDoS attacks. In [24], the authors addressed signaling storms attacks that can lead to Denial of Service (DoS), exploiting the Open RAN architecture. The authors periodically rebooted the antennas of compromised O-RUs to generate several handover events. All these works leveraged AI/ML to detect the attacks.

While these papers provide early detection of DDoS and signaling-related threats, our work complements them by focusing on user-plane DDoS detection within a 3GPP-aligned NWDAF scenario, using an open-source dataset captured over-the-air in a live 5G testbed. Additionally, we incorporate SHAP-based explainability to enhance the transparency of closed-box model decisions, particularly in consumer-centric 6G use cases.

This work builds on the use of a domain-specific dataset that captures dynamic traffic patterns and DDoS attacks initiated by malicious User Equipments (UEs) against a 5G live network. We study the development of deep learning models, including

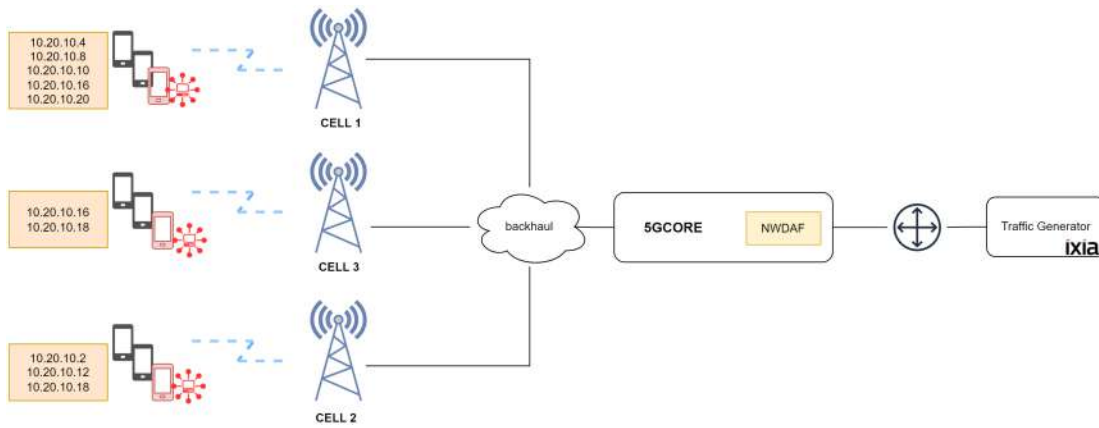


Fig. 1. Testbed setup [3].

TABLE I
SUMMARY OF TRAFFIC EVENTS IN THE DATASET [3], [5]

Event Type	Date Observed	Duration of Event (UTC)	IPs
SYN Flood	18-Aug-2024	07:00–08:00	10.20.10.2, 10.20.10.4
ICMP Flood	19-Aug-2024	07:00–09:41	10.20.10.2, 10.20.10.4
UDP Fragmentation	19-Aug-2024	17:00–18:00	10.20.10.2, 10.20.10.4
DNS Flood	21-Aug-2024	12:00–13:00	10.20.10.2, 10.20.10.4
GTP-U Flood	21-Aug-2024	17:00–18:00	10.20.10.2, 10.20.10.4, 10.20.10.6, 10.20.10.8, 10.20.10.10
Streaming (Benign Traffic: Skype, YouTube)	17–21-Aug-2024	Start: 16:00 (17-Aug) End: 20:00 (21-Aug)	10.20.10.12, 10.20.10.16, 10.20.10.18, 10.20.10.20

CNNs, LSTMs, and MLPs, as well as the use of XGBoost, to detect these DDoS attacks. During our study, we optimized the architecture of the deep learning models, employed the Focal Loss function and used Synthetic Minority Over-sampling Technique (SMOTE) for their training to address the imbalanced traffic patterns and ensure high detection accuracy and recall. We used dynamic learning rate during training to ensure stable convergence of the models' loss functions. Section IV describes in detail the selection of these parameters. Our work enhances anomaly detection but also provides a scalable foundation for securing emerging consumer applications, such as immersive experiences and autonomous services, aligned with the demands of B5G and 6G networks.

The development and standardization of datasets reflecting next-generation network behaviors will be instrumental in advancing the field. Such efforts, combined with ongoing model innovations using Digital Twins [25], will provide the robust, scalable, and secure AI systems needed to support the future of telecommunications. Our approach demonstrates how tailored datasets can enhance the reliability and efficiency of anomaly detection, ensuring secure and resilient operations in the next generation of networks.

III. METHODOLOGY AND EXPERIMENTAL SETUP

Fig. 1 [3] depicts the testbed topology, comprising three cells supporting nine UEs connected to a 5G core network. The network is implemented using the Amarisoft Callbox Mini

solution, supplemented by two additional cells from Amarisoft Classic, which also hosts the 5G core [26].

In line with the 3GPP technical specifications for the detection of abnormal UE behavior [4] using the NWDAF, this study investigates DDoS attacks by capturing and openly sharing control signaling metrics from a 5G network that can help identify such attacks from malicious UEs. The DDoS attacks performed include SYN, ICMP and GTP flood attacks, and UDP fragmentation.

Table I summarizes the benign and malicious events taking place through the dataset recording, alongside the IPs of the UEs initiating each traffic type. SYN Flood attacks sent TCP SYN packets with a data size of 120 bytes and a window size of 64 to port 80, aiming to exhaust connection slots. ICMP Flood overloaded the target with 120-byte ICMP packets to port 80, creating excessive traffic. UDP Fragmentation fragmented UDP packets to evade detection and strain memory buffers. DNS Flood targeted the DNS server on port 53 with randomized source addresses to saturate the service. The GTP-U Flood Attack sends malformed GTP-U packets in the N6 network interface of the 5G Core (port 2152) [27].

Fig. 2 illustrates the boxplot of the uplink (UL) bitrate for malicious and benign UEs. Malicious UEs display limited variability within the inter-quartile range, reflecting the steady and repetitive nature of the traffic used in the attacks. In contrast, benign UEs show broader variation in UL bitrate, consistent with typical user behavior in streaming applications such as Skype and YouTube.

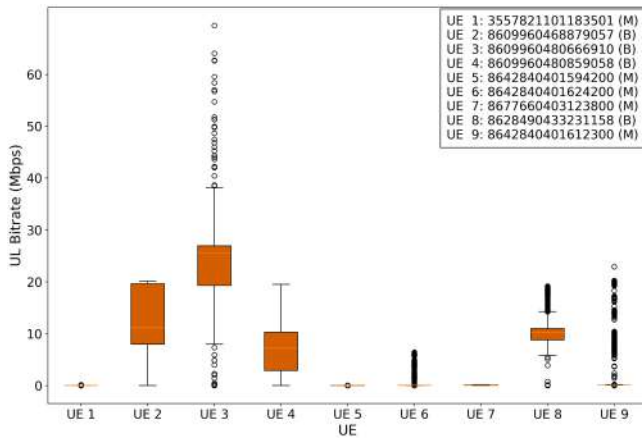


Fig. 2. Boxplot of the UL Bitrate of malicious and benign UEs. The malicious UEs exhibit lack of variability within the inter-quartile range, highlighting the traffic profile used in the attacks. The benign UEs showcase variable UL bitrate, because of their streaming applications, *i.e.*, Skype and YouTube.

The data set is collected through a data collector that interfaces with the 5G network, capturing data from UEs, gNodeBs (gNBs), and the Core Network from three different cells. Each UE was associated with one of three cells, and the relevant cell-specific features were consolidated into unified columns based on the UE’s associated cell. Known attack windows (e.g., SYN flood, ICMP flood) were defined, and data points within these intervals were flagged with a binary attack label. The preprocessed data are stored in three files: “amari_ue_data.csv,” “enb_counters.csv,” [28], and “mme_counters.csv.” The complete dataset and its summary report can be found in [5]. Due to space constraints, we focus on “amari_ue_data.csv,” which includes UE IDs, IP addressing, bearer, and cell information alongside downlink and uplink bitrates. We provide a description of the most significant features, which are the ones that impact the decision of the machine learning models, in Section IV.

IV. EXPERIMENTAL RESULTS

The following subsections describe the design, optimizations and results of a Convolutional Neural Network (CNN), a Long Short-Term Memory (LSTM) network, a Multi-layer Perceptron (MLP), and XGBoost, an ensemble of weak learners, that is compared to neural networks. We also compare the results against Z-Score, a traditional statistical method, used in [3] on the same dataset.

We frame the problem as a binary classification task, where the model is trained to distinguish between malicious and benign samples. We have used cross-validation to train the models.

We used SHAP to calculate the contribution of each feature to the model’s predictions by analyzing the impact of the feature across all possible subsets of features. Formula 1 is calculating the SHAP value of the feature’s contribution.

$$\phi_i = \sum_{S \subseteq \{1, \dots, M\} \setminus \{i\}} \frac{|S|!(M - |S| - 1)!}{M!} [v(S \cup \{i\}) - v(S)] \quad (1)$$

TABLE II
TRAINING FEATURES DESCRIPTIONS [29]

Feature	Description
ul_retx	Number of received uplink transport blocks with CRC errors.
dl_retx	Number of downlink retransmitted transport blocks.
ul_tx	Number of received uplink transport blocks (without CRC error).
dl_tx	Number of downlink transmitted transport blocks (without retransmissions).
ul_bitrate	Uplink bitrate in bits per seconds.
dl_bitrate	Downlink bitrate in bits per seconds.
ul_mcs	Average uplink MCS.
dl_mcs	Average downlink MCS.
ul_path_loss	Last computed UL path loss in dB, estimated from power headroom report.
cell_id	Cell ID.
tac	Tracking Area Code.
epre	Last received EPRE in dBm.
turbo_decoder_avg	Average turbo/ldpc decoder pass.
initial_ta	Description of ‘initial_ta’.
bearer_0_session_id	Session ID of Bearer 0.
bearer_1_session_id	Session ID of Bearer 1.
bearer_0_dl_total_bytes	Total downlink PDCP SDU byte count.
bearer_0_qos_flow_id	QoS flow identifier allocated to bearer 0.
bearer_0_sst	Slice Service Type.
bearer_0_ul_total_bytes	Total uplink PDCP SDU byte count.
bearer_1_dl_total_bytes	Total downlink PDCP SDU byte count.
bearer_1_qos_flow_id	QoS flow identifier allocated to bearer 1.
bearer_1_sst	Slice Service Type.
bearer_1_ul_total_bytes	Total uplink PDCP SDU byte count.
t3512	AMF provides this timer value to UE in the Registration Accept message.
ue_aggregate_max_bitrate_dl	UE aggregate maximum bitrate for downlink (in bits/s).
ue_aggregate_max_bitrate_ul	UE aggregate maximum bitrate for uplink (in bits/s).
ul_err	Number of non received uplink transport blocks (after retransmissions).
ul_n_layer	Uplink layer count.
ul_phr	Last received power headroom report.
ul_rank	Last uplink rank computed by the gNB in NR cells.
dl_err	Number of downlink non transmitted transport blocks (after retransmissions).
cqi	Channel Quality Indicator.
p_ue	UE transmission power in dB, estimated from PHR and Pmax set in the cell and reported by UE.
pusch_snr	Last received PUSCH Signal to Noise Ratio.
ri	Rank Indicator (number of layers for MIMO).
turbo_decoder_max	Maximum turbo/ldpc decoder pass.
turbo_decoder_min	Minimum turbo/ldpc decoder pass.

Explanation:

- ϕ_i : The SHAP value for feature i , representing its contribution to the model’s prediction.
- M : Total number of features.
- S : A subset of features excluding i (*i.e.*, $S \subseteq \{1, \dots, M\} \setminus \{i\}$).
- $v(S)$: The model’s value (e.g., expected prediction) when using only the features in subset S .
- $v(S \cup \{i\}) - v(S)$: The marginal contribution of feature i when added to subset S .

- $\frac{|S|!(M-|S|-1)!}{M!}$: A weighting factor that ensures fair contribution of feature i across all possible subsets S .

$$\text{Feature importance for feature } i = \mathbb{E}[|\phi_i|] = \frac{1}{N} \sum_{j=1}^N |\phi_i^{(j)}| \quad (2)$$

Explanation:

- $\mathbb{E}[|\phi_i|]$: The mean absolute SHAP value for feature i , representing its overall importance.
- N : The total number of instances in the dataset.
- $\phi_i^{(j)}$: The SHAP value of feature i for instance j , quantifying its contribution to the model's prediction for that instance.
- $|\phi_i^{(j)}|$: The absolute value of the SHAP value for feature i , ignoring the direction (positive or negative) of its contribution.

For handling class imbalance, we employed the Focal Loss function:

$$FL(p_t) = -\alpha_t(1 - p_t)^\gamma \log(p_t), \quad (3)$$

where p_t is the model's confidence in the true class, α_t is a weighting factor that balances the importance of classes, and γ is a focusing parameter that reduces the loss contribution from well-classified examples. By dynamically scaling the loss contribution of each sample based on its classification difficulty, Focal Loss ensures that the network learns effectively even in the presence of severe class imbalance.

For the Neural Network models, input features were scaled using StandardScaler. The models are trained using the AdamW optimizer, which enhances the Adam optimization algorithm by decoupling weight decay from the gradient updates. The optimization process is expressed as:

$$\theta_{t+1} = \theta_t - \eta \left(\frac{m_t}{\sqrt{v_t + \epsilon}} + \lambda \theta_t \right), \quad (4)$$

where η is the learning rate, m_t and v_t are the first and second moment estimates, and λ represents the weight decay coefficient. The learning rate used was $1e-4$ and the weight decay was $1e-4$.

A. Convolutional Neural Network (CNN)

A one-dimensional Convolutional Neural Network (1D CNN) was developed to address the binary classification task on a dataset comprising 38 features. This architecture leverages the ability of CNNs to hierarchically extract features from input data, making them highly effective for anomaly detection in network traffic. The model's architecture was meticulously designed to ensure both robustness and interpretability, while addressing the challenges posed by imbalanced datasets.

The CNN begins with two convolutional layers, which serve as the backbone of the hierarchical feature extraction process. Each convolutional layer is followed by Batch Normalization to stabilize training, mitigate the internal covariate shift, and accelerate convergence. These layers extract localized patterns from the input data, which are critical for distinguishing between benign and malicious traffic. ReLU (Rectified Linear

Unit) activation functions are employed within each layer to introduce non-linearity, enabling the network to capture complex interactions between features. To reduce the spatial dimensions and computational complexity, Max Pooling layers are applied after each convolutional layer. This operation not only downsamples the feature maps but also helps in retaining the most significant patterns from the input data.

Formally, given an input feature vector $\mathbf{x} \in \mathbb{R}^d$, the convolutional layers apply a set of filters \mathbf{w} of size k to compute feature maps as follows:

$$\mathbf{z}[i] = \sigma \left(\sum_{j=0}^{k-1} \mathbf{w}[j] \cdot \mathbf{x}[i+j] + b \right), \quad (5)$$

where $\sigma(\cdot)$ denotes the ReLU activation function, and b is a bias term. The combination of convolution and activation ensures that the network captures both low-level and high-level features essential for classification.

To mitigate overfitting, a Dropout layer is incorporated after the convolutional operations. This layer randomly deactivates neurons during training, which helps in preventing the model from relying excessively on specific features. The fully connected (dense) layers follow the convolutional layers, reducing the high-dimensional feature maps to binary predictions. Specifically, the first dense layer consists of 128 neurons, with subsequent layers progressively reducing dimensionality. The output layer employs a softmax activation function:

$$\hat{y} = \text{softmax}(\mathbf{W}\mathbf{h} + \mathbf{b}), \quad (6)$$

where \mathbf{h} represents the flattened output from the final convolutional layer, and \mathbf{W} , \mathbf{b} are the learned weights and biases of the dense layers. The softmax function ensures that the output probabilities sum to 1, facilitating binary classification.

The AdamW optimizer, as defined in Equation (4), is used to train the model.

To address the class imbalance inherent in the dataset, the Focal Loss function was employed. Focal Loss modifies the standard cross-entropy loss to prioritize the minority class and down-weight the contribution of well-classified examples. It is defined as the Equation (3), where $\alpha_t = 0.25$ and $\gamma = 2.0$.

The preprocessing pipeline incorporates the Synthetic Minority Oversampling Technique (SMOTE) to further address class imbalance. SMOTE generates synthetic samples for the minority class by interpolating between existing samples. This technique helps in creating a balanced dataset without introducing noise. The dataset is divided into training, validation, and test sets, ensuring that the model is evaluated on unseen data to assess its generalization capabilities. The architecture is trained over multiple epochs, with the validation set providing feedback to prevent overfitting and fine-tune hyperparameters.

Performance metrics such as precision, recall, F1-score, and accuracy, as reported in Table III, are used to evaluate the CNN model. The CNN achieves a weighted F1-score of 0.93, with a precision of 0.91 and recall of 0.95 for the attack class, indicating strong sensitivity to malicious traffic. The decision threshold for binary classification is optimized to balance precision and recall, which is particularly important

TABLE III

COMPARISON OF CNN, LSTM, MLP, AND XGBOOST CLASSIFICATION MODELS ACROSS MULTIPLE METRICS. PRECISION (0): ACCURACY OF PREDICTING NO ATTACK. PRECISION (1): ACCURACY OF PREDICTING ATTACKS. RECALL (0): ABILITY TO DETECT NON-ATTACKS CORRECTLY. RECALL (1): ABILITY TO DETECT ATTACKS CORRECTLY. F1 (0): BALANCE OF PRECISION AND RECALL FOR NO ATTACK. F1 (1): BALANCE OF PRECISION AND RECALL FOR ATTACKS

Model	Accuracy	Precision (0)	Recall (0)	F1 (0)	Precision (1)	Recall (1)	F1 (1)	Weighted F1
Z-Score Method [3]	0.919	0.96	0.96	0.96	0.33	0.31	0.32	0.32
CNN	0.931	0.95	0.91	0.93	0.91	0.95	0.93	0.93
LSTM	0.900	0.94	0.85	0.90	0.87	0.95	0.91	0.90
MLP	0.907	0.93	0.88	0.90	0.89	0.94	0.91	0.91
XGBoost	0.996	1.00	1.00	1.00	0.96	0.98	0.97	1.00

for anomaly detection tasks where minimizing false negatives is critical.

To enhance the interpretability of the CNN model, SHAP (SHapley Additive exPlanations) analysis is applied. SHAP provides a detailed breakdown of the contribution of each feature to the model's predictions, enabling a deeper understanding of the decision-making process. The Fig. 4 (a) reveals that features such as `ul_retx` (uplink retransmissions) and `dl_tx` (downlink transmissions) are particularly influential. For example, higher values of `ul_retx` strongly push predictions toward the positive class, indicating its importance in identifying anomalous behavior. Similarly, elevated values of `dl_tx` are associated with a higher likelihood of anomaly classification. These insights demonstrate the value of domain-specific features in improving the reliability and robustness of AI-driven anomaly detection systems.

In summary, the 1D CNN model effectively captures hierarchical representations of network traffic data. Through the combination of advanced preprocessing techniques, robust architectural design, and interpretability tools such as SHAP, the model achieves high performance in detecting anomalies, even in the presence of class imbalance. This demonstrates its potential as a reliable tool for predictive security in next-generation networks.

B. LSTM

We developed a Long Short-Term Memory (LSTM) neural network for binary classification on a dataset containing 38 features. LSTM networks were chosen for their ability to retain memory across time steps. DDoS attacks often exhibit temporal behavior, such as sustained retransmissions or bitrate shifts. LSTMs can capture these evolving patterns better than feedforward models. The architecture consists of a two-layer LSTM module, where each layer contains 64 hidden units. The memory cell of the LSTM is defined by the following equations:

$$\mathbf{i}_t = \sigma(\mathbf{W}_i \mathbf{x}_t + \mathbf{U}_i \mathbf{h}_{t-1} + \mathbf{b}_i), \quad (7)$$

$$\mathbf{f}_t = \sigma(\mathbf{W}_f \mathbf{x}_t + \mathbf{U}_f \mathbf{h}_{t-1} + \mathbf{b}_f), \quad (8)$$

$$\mathbf{o}_t = \sigma(\mathbf{W}_o \mathbf{x}_t + \mathbf{U}_o \mathbf{h}_{t-1} + \mathbf{b}_o), \quad (9)$$

$$\tilde{\mathbf{c}}_t = \tanh(\mathbf{W}_c \mathbf{x}_t + \mathbf{U}_c \mathbf{h}_{t-1} + \mathbf{b}_c), \quad (10)$$

$$\mathbf{c}_t = \mathbf{f}_t \odot \mathbf{c}_{t-1} + \mathbf{i}_t \odot \tilde{\mathbf{c}}_t, \quad (11)$$

$$\mathbf{h}_t = \mathbf{o}_t \odot \tanh(\mathbf{c}_t), \quad (12)$$

where $\mathbf{i}_t, \mathbf{f}_t, \mathbf{o}_t$ represent the input, forget, and output gates, respectively, and \mathbf{c}_t denotes the cell state. The input at timestep t is \mathbf{x}_t , and \mathbf{h}_{t-1} is the hidden state from the previous timestep. The weight matrices $\mathbf{W}_i, \mathbf{W}_f, \mathbf{W}_o, \mathbf{W}_c$ and bias vectors $\mathbf{b}_i, \mathbf{b}_f, \mathbf{b}_o, \mathbf{b}_c$ are learned parameters. The element-wise multiplication operator is denoted by \odot , and $\sigma(\cdot)$ is the sigmoid activation function.

To stabilize training and improve generalization, Batch Normalization is applied to the final hidden state output of the LSTM layers. This normalization reduces internal covariate shifts and ensures a smoother optimization landscape. The processed output is then passed through fully connected layers with ReLU activations, which progressively reduce the dimensionality to the final binary classification output. Dropout layers are incorporated between fully connected layers to prevent overfitting by randomly deactivating neurons during training.

The model is trained using the AdamW optimizer defined as the Equation (4).

The training process is optimized using the Focal Loss function, expressed as the Equation (3), where $\alpha_t = 0.25$ and $\gamma = 2.0$.

To further balance the dataset, we employ the Synthetic Minority Oversampling Technique (SMOTE), which generates synthetic samples by interpolating between existing samples of the minority class. This approach mitigates class imbalance and improves the model's ability to generalize. The learning rate is adjusted dynamically during training using a StepLR scheduler, which reduces the learning rate by a factor of 0.5 after every five epochs. This strategy ensures stable convergence by allowing finer adjustments to the model parameters as training progresses.

The dataset is divided into training, validation, and test sets to monitor the model's performance at different stages and to avoid overfitting. Evaluation metrics, including classification reports, precision-recall curves, and threshold-optimized F1 scores, are used to comprehensively assess the model's effectiveness. As shown in Table III, the LSTM achieves a weighted F1-score of 0.90, with a recall of 0.95 and F1-score of 0.91 for the attack class, demonstrating its ability to capture sequential malicious behavior. This architecture is particularly well-suited for imbalanced sequential data, delivering high accuracy and robustness.

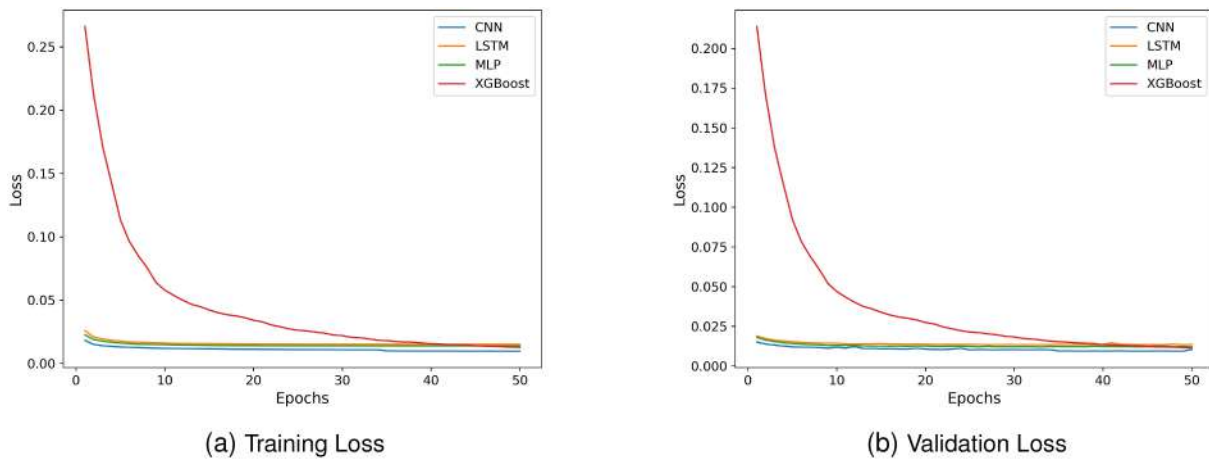


Fig. 3. The training and validation loss plots for CNN, LSTM, MLP and XGBoost.

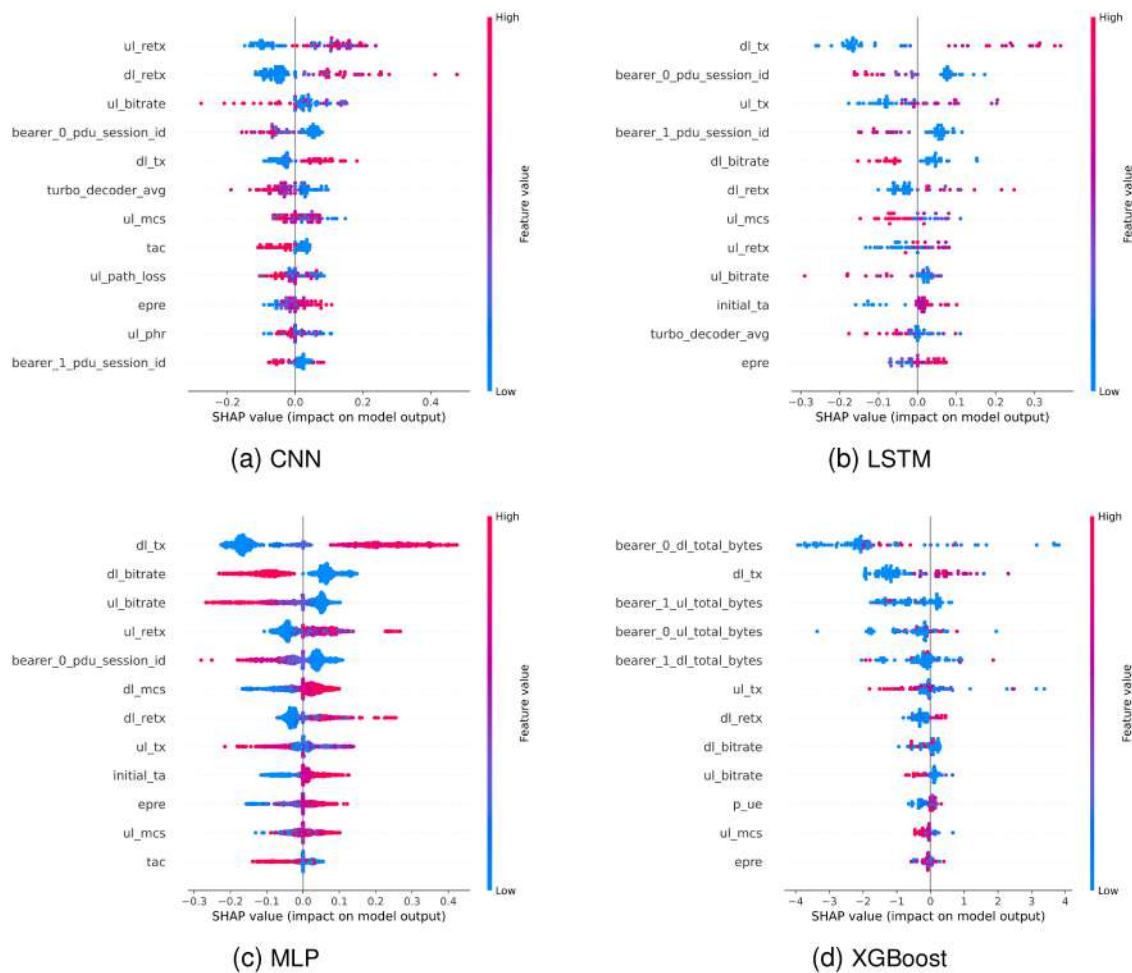


Fig. 4. SHAP beeswarm plot showing the top 12 features by their impact on the model predictions.

To enhance interpretability, we utilized SHAP (SHapley Additive exPlanations) to analyze the contributions of individual features to the LSTM model’s predictions. SHAP assigns a value to each feature based on its impact on the model’s output. The Fig. 4 (b) reveals that features such as `dl_tx` (downlink transmissions) and `bearer_0_pdu_session_id` were identified as having significant contributions. The feature

`bearer_0_pdu_session_id`, representing the session ID of bearer 0 used for data transmission, is particularly indicative of abnormal activity during DDoS attacks. Elevated values of `dl_tx` strongly correlate with positive predictions, as shown by their high SHAP values, which push predictions toward the positive class. Conversely, lower SHAP values (blue) decrease the likelihood of classifying an observation as an anomaly.

The loss plot for the training and validation phases of the LSTM model is presented in Fig. 3, highlighting the steady reduction in loss and convergence over epochs. These plots provide a visual representation of the model's learning dynamics, further validating its robustness.

In summary, the LSTM model effectively captures temporal dependencies within the data and addresses the challenges of imbalanced datasets through advanced loss functions, preprocessing techniques, and dynamic learning rate adjustments. The integration of SHAP enhances interpretability, providing actionable insights into the key drivers of anomaly classification.

C. Multi-Layer Perceptron (MLP)

We implemented a Multi-Layer Perceptron (MLP) neural network for binary classification on a dataset with 38 features. The MLP is a feed-forward neural network architecture that processes input features through successive fully connected layers. This design enables the model to learn complex, non-linear relationships within the data. The network architecture consists of four fully connected layers, with hidden dimensions progressively reducing from 256 to 128, 64, and finally to 2 output neurons, which represent the binary classification output. The reduction in dimensionality ensures that the network captures hierarchical feature representations while preventing overfitting. The output layer employs a softmax activation function to compute class probabilities:

$$\hat{y} = \text{softmax}\left(\mathbf{W}^{(L)}\mathbf{h}^{(L-1)} + \mathbf{b}^{(L)}\right), \quad (13)$$

where $\mathbf{h}^{(L-1)}$ is the output from the last hidden layer, $\mathbf{W}^{(L)}$ and $\mathbf{b}^{(L)}$ are the learned weights and biases of the final layer, and \hat{y} represents the predicted class probabilities.

For each hidden layer l , the output is computed as:

$$\mathbf{h}^{(l)} = \sigma\left(\mathbf{W}^{(l)}\mathbf{h}^{(l-1)} + \mathbf{b}^{(l)}\right), \quad (14)$$

where $\sigma(\cdot)$ is the ReLU activation function, $\mathbf{W}^{(l)}$ and $\mathbf{b}^{(l)}$ are the weight and bias matrices for layer l , and $\mathbf{h}^{(l-1)}$ is the input to layer l . The ReLU activation introduces non-linearity, allowing the network to capture complex patterns in the data.

To ensure stability and convergence during training, Batch Normalization is applied after the first two fully connected layers. This technique normalizes the layer inputs by adjusting their mean and variance across the mini-batch, as defined by:

$$\mathbf{z}_{\text{norm}} = \frac{\mathbf{z} - \mu}{\sqrt{\sigma^2 + \epsilon}}, \quad (15)$$

where μ and σ^2 are the batch mean and variance, respectively, and ϵ is a small constant added for numerical stability. Batch Normalization accelerates training convergence and mitigates internal covariate shift.

To further reduce overfitting, a Dropout layer with a rate of 0.3 is applied after each hidden layer. During training, Dropout randomly sets a fraction p of the neurons to zero, ensuring that the network does not rely excessively on specific features.

Training is performed using the AdamW optimizer, described in Equation (4).

To handle the class imbalance inherent in the dataset, the Focal Loss function is employed. This loss function dynamically adjusts the contribution of each sample based on the model's confidence in its prediction. The Focal Loss is mathematically expressed as the Equation (3), where $\alpha_t = 0.25$ and $\gamma = 2.0$.

To further address class imbalance, we applied the Synthetic Minority Oversampling Technique (SMOTE), which generates synthetic samples for the minority class by interpolating between existing samples. This technique enhances the representation of the minority class without introducing noise. The dataset is divided into training, validation, and testing subsets. The validation set is used for hyperparameter tuning and overfitting monitoring, while the test set evaluates the model's generalization performance.

Performance is evaluated using precision-recall analysis, which is particularly effective for imbalanced datasets. An optimal decision threshold is identified to maximize the balance between precision and recall, ensuring reliable classification of minority samples. As reported in Table III, the MLP achieves a weighted F1-score of 0.91, with a recall of 0.94 and F1-score of 0.91 for the attack class, confirming its effectiveness in detecting malicious traffic.

To enhance interpretability, we employed SHAP to analyze the feature contributions to the model's predictions. SHAP assigns a value to each feature based on its impact on the predicted outcome. For instance, `dl_tx` (downlink transmissions) was identified as a key feature, with higher values (red) pushing predictions toward the positive class, as illustrated by their strong positive SHAP values. Similarly, in Fig. 4 (c), `dl_bitrate` (downlink bitrate) showed a significant positive contribution to the model's predictions, with higher feature values increasing the likelihood of anomaly detection. Conversely, lower SHAP values (blue) for these features reduced the probability of a positive classification.

The MLP model effectively learns complex relationships within the dataset while addressing the challenges of class imbalance through advanced loss functions and preprocessing techniques. By leveraging SHAP for interpretability, the model provides actionable insights into the key drivers of its predictions, enhancing its reliability and robustness for binary classification tasks.

D. XGBOOST

We developed an XGBoost model for binary classification on a dataset with 38 features. XGBoost is a gradient boosting framework that builds an ensemble of decision trees to optimize performance on tabular data. To address the class imbalance inherent in the dataset, we employed a custom undersampling strategy, reducing the majority class while retaining all minority class samples. This ensures that the model focuses equally on both classes during training.

The dataset underwent preprocessing steps including imputation of missing values, label encoding of categorical variables, and feature scaling using StandardScaler to normalize feature distributions. For further balance, we applied random undersampling with a custom sampling strategy. The

model was trained with logloss as the evaluation metric, ensuring robust optimization of probabilities for binary classification. To prevent overfitting, early stopping rounds were configured, monitoring validation performance during training.

Hyperparameters such as `scale_pos_weight` were tuned to emphasize the minority class, ensuring the model is sensitive to underrepresented samples. In addition, the tree-based structure of XGBoost automatically captures feature interactions, making it highly effective for complex decision boundaries. The evaluation included metrics like accuracy, F1-score, precision-recall curves, and ROC AUC. As shown in Table III, XGBoost achieves the highest overall performance, with an accuracy of 0.996, a recall of 0.98, and an F1-score of 0.97 for the attack class, as well as a weighted F1-score of 1.00. Overall, XGBoost showcases the best performance among the selected models, both in terms of predictive accuracy and training efficiency.

Based on Fig. 4 (d), for `bearer_0_dl_total_bytes`, high values (red) significantly increase, pushing predictions toward the positive class, indicating potential attacks. For `dl_tx`, high values (red) similarly have a strong positive impact on predictions, while low values (blue) reduce the likelihood of an attack, as shown by their SHAP values on the x-axis.

E. Discussion

While this work demonstrates the feasibility of AI/ML-based DDoS detection in 5G environments, some aspects need to be further studied. While the dataset was recorded on a real 5G testbed, it focuses on DDoS attacks, which may constrain model generalisation. Future datasets will incorporate a broader spectrum of attack models, including application layer attacks, protocol specific exploits, and attacks against the 5G interfaces (e.g., N2, N6, N11) and Core Network Functions (e.g., AMF, SMF). Furthermore, considerations for real-time deployment, such as inference latency, resource constraints at the edge, and model adaptability, remain important for applying these methods in practical B5G/6G scenarios. Specifically, it is also worth noting that the decision threshold in the real-time detection setting shows a degree of instability, which may affect the model's consistency in classifying borderline cases and should be considered when deploying in dynamic environments. The broader question of robustness under adversarial or noisy conditions lies beyond the scope of this study and remains open for future exploration.

Among the evaluated models, XGBoost demonstrates the highest overall performance, achieving near-perfect scores across all metrics, including an accuracy of 0.996, precision and recall of 1.00 for the benign class, and a weighted F1-score of 1.00. Its strong performance, particularly in detecting the minority (attack) class with a recall of 0.98, and F1 of 0.97, indicates a high degree of sensitivity to malicious traffic. This is further supported by the relatively lower recall values of the deep learning models (ranging from 0.94 to 0.95), suggesting that XGBoost is more effective at minimizing false negatives, which is a critical requirement in security-focused applications. Compared to deep learning models, XGBoost

offers a more balanced precision-recall trade-off without the added training complexity.

V. CHALLENGES IN FUTURE-PROOFING CONSUMER APPLICATIONS

A. Ensuring Real-Time Anomaly Detection in Consumer-Centric Applications

Consumer applications in B5G/6G networks, such as AR/VR gaming, smart home automation, and autonomous transportation, require ultra-low latency and high availability to ensure seamless user experiences. AI-driven anomaly detection must operate within strict time constraints to prevent service disruptions caused by cyber threats like DDoS attacks or unauthorized access. However, the challenge lies in designing lightweight yet effective AI/ML models that can process vast amounts of network traffic in real-time while running on resource-constrained edge devices. Traditional AI approaches often require significant computational power, leading to potential bottlenecks that impact responsiveness. Future research must focus on optimizing model architectures, leveraging edge AI for on-device inference, and integrating with real-time analytics platforms to maintain security without compromising application performance.

B. Dataset Limitations for Consumer Application Security

The effectiveness of AI-driven security solutions heavily depends on the quality and diversity of training datasets. While existing datasets capture some attack scenarios in telecom networks, there is a lack of comprehensive, domain-specific datasets that reflect real-world threats targeting consumer applications. For instance, datasets should include adversarial behaviors in smart home devices, data breaches in personal cloud storage, and attacks on wearable health devices to improve anomaly detection accuracy. Furthermore, the specialization of datasets in emerging attack vectors unique to 6G, such as AI-driven cyber threats and quantum-enabled attacks. The challenge is not only in data collection but also in maintaining privacy, ensuring annotation consistency, and integrating real-world consumer traffic patterns without violating user confidentiality. Future efforts should focus on creating open, labeled datasets that balance representativeness, scalability, and compliance with data protection regulations.

C. Personalization vs. Privacy in AI-Based Security

As consumer applications increasingly rely on AI-driven security solutions, there is a growing need to personalize threat detection while preserving user privacy. Personalization enhances security by tailoring anomaly detection to individual user behaviors, such as recognizing deviations in smart home automation patterns or detecting unusual financial transactions. However, collecting and analyzing such personal data introduces privacy risks, as AI models could inadvertently expose sensitive information if mishandled. Federated learning and homomorphic encryption offer potential solutions by enabling AI models to learn from decentralized user data without directly accessing it. The challenge is striking a balance between security effectiveness and privacy preservation,

ensuring compliance with regulations such as GDPR while maintaining accurate, real-time threat detection in consumer environments.

D. Integration With Next-Generation Network Architectures

For AI-driven security to be effective in consumer applications, it must seamlessly integrate with next-generation network functions, including the Network Data Analytics Function (NWDAF) in 5G and future 6G security frameworks. NWDAF enables real-time data analytics within the core network, but its full potential remains underutilized in consumer security applications. A key challenge is ensuring that AI-based anomaly detection systems can interact with NWDAF and other service-based architecture components to proactively mitigate threats without adding excessive latency. Furthermore, AI models should be deployed at multiple network layers, from the cloud to the edge, to optimize security enforcement in decentralized environments. Future research should explore federated AI frameworks, distributed threat intelligence sharing, and real-time coordination between network entities to enhance security resilience while maintaining low overhead for consumer-facing applications.

E. Balancing Security With Quality of Experience (QoE)

AI-driven security mechanisms must ensure robust protection against cyber threats without degrading the user experience of consumer applications. A high rate of false positives in anomaly detection can lead to unnecessary security interventions, such as blocking legitimate network traffic or triggering excessive authentication requests, causing frustration for end-users. Conversely, false negatives—missed detections—can result in security breaches that compromise personal data or disrupt critical services. Achieving this balance requires advanced AI techniques that can dynamically adjust sensitivity thresholds based on contextual factors such as user location, historical behavior, and network congestion. Additionally, adaptive security frameworks that prioritize QoE must be integrated with self-learning AI models capable of minimizing disruptions while maintaining high detection accuracy.

VI. CONCLUSION

This study explored AI-driven anomaly detection for consumer applications in 5G/6G networks, focusing on detecting DDoS attacks using a real-world 5G testbed dataset. By evaluating deep learning models (CNNs, LSTMs, MLPs) alongside XGBoost, results demonstrated XGBoost as the most efficient and accurate approach for real-time security. SHAP analysis provided insight into key network features influencing model decisions, enhancing interpretability.

Future work should expand the dataset to include a broader range of cyber threats, such as adversarial AI, protocol specific attacks, and supply chain attacks, ensuring models generalize across diverse consumer applications and attack models. Additionally, improving real-time deployment, considering classification threshold instability across time, model explainability, and privacy-preserving techniques will be essential

for developing scalable and trustworthy AI-driven security solutions in next-generation networks.

ACKNOWLEDGMENT

Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the EU or SNS JU.

REFERENCES

- [1] K. Singh, P.-C. Wang, S. Biswas, S. K. Singh, S. Mumtaz, and C.-P. Li, "Joint active and passive beamforming design for RIS-aided IBFD IoT communications: QoS and power efficiency considerations," *IEEE Trans. Consum. Electron.*, vol. 69, no. 2, pp. 170–182, May 2023.
- [2] M. U. Hashmi et al., "Concomitant skew and phase correction (CSPC) for industry 5.0 enabler pervasive distributed computing systems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1511–1518, Feb. 2024.
- [3] M. Christopoulou et al., "User terminals as attackers: An open dataset analysis of DDoS attacks in 5G networks," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2024, pp. 301–307.
- [4] *Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services, Release 18, Version 18.4.0*, 3GPP Standard TS 23.288, Dec. 2023.
- [5] (Space Hellas, Greece, Balkans). *NCSR-D5-5GDDoS: 5G Radio and Core Metrics Containing Sporadic DDoS Attacks: National Centre of Scientific Research Demokritos*. (2024). [Online]. Available: <https://doi.org/10.5281/zenodo.13900057>
- [6] M. Liyanage et al., "Advancing security for 6G smart networks and services," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, 2024, pp. 1169–1174.
- [7] H. W. Olewi, D. N. Mhawi, and H. Al-Raweshdy, "MLTs-ADCNs: Machine learning techniques for anomaly detection in communication networks," *IEEE Access*, vol. 10, pp. 91006–91017, 2022.
- [8] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," in *Proc. 2nd Int. Conf. Comput. Sci. Artif. Intell.*, 2018, pp. 81–85.
- [9] A. Rosay, E. Cheval, F. Carlier, and P. Leroux, "Network intrusion detection: A comprehensive analysis of CIC-IDS2017," in *Proc. 8th Int. Conf. Inf. Syst. Secur. Privacy*, 2022, pp. 25–36.
- [10] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Comput. Netw.*, vol. 174, Jun. 2020, Art. no. 107247.
- [11] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly detection in 6G networks using machine learning methods," *Electronics*, vol. 12, no. 15, p. 3300, 2023.
- [12] Y. Zhao, C. Hu, and R. Wang, "Support vector machine (SVM) to predict risk factors in the 6G cyber digital transformation process of enterprises," *Wireless Pers. Commun.*, pp. 1–18, Apr. 2024, doi: [10.1007/s11277-024-11020-7](https://doi.org/10.1007/s11277-024-11020-7).
- [13] R. A. A. Habeeb, F. Nasaruddin, A. Gani, I. A. T. Hashem, E. Ahmed, and M. Imran, "Real-time big data processing for anomaly detection: A survey," *Int. J. Inf. Manage.*, vol. 45, pp. 289–307, Apr. 2019.
- [14] O. Rippel, P. Mertens, and D. Merhof, "Modeling the distribution of normal data in pre-trained deep features for anomaly detection," in *Proc. 25th Int. Conf. Pattern Recognit. (ICPR)*, 2021, pp. 6726–6733.
- [15] W. Wang, X. Zhang, S. Gombault, and S. J. Knapkog, "Attribute normalization in network intrusion detection," in *Proc. 10th Int. Symp. Pervasive Syst., Algorithms, Netw.*, 2009, pp. 448–453.
- [16] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, 2015, pp. 1–6.
- [17] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, 2019, pp. 1–8.
- [18] V. Hnamte, A. A. Najjar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Comput. Security*, vol. 138, Mar. 2024, Art. no. 103661.
- [19] "SNS GA-101096110 JU privateer: Privacy-first security enablers for 6G networks: Privateer consortium." 2024, Accessed: Mar. 6, 2025. [Online]. Available: <https://www.privateer-project.eu/>

- [20] N.-N. Dao et al., "A review on new technologies in 3GPP standards for 5G access and beyond," *Comput. Netw.*, vol. 245, May 2024, Art. no. 110370.
- [21] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," *Syst. Sci. Control Eng.*, vol. 12, no. 1, 2024, Art. no. 2321381.
- [22] L. Abdelrazek, R. Fuladi, J. Kövér, L. Karaçay, and U. Gülen, "Detecting IP DDoS attacks using 3GPP radio protocols," *IEEE Access*, vol. 12, pp. 24776–24790, 2024.
- [23] B. M. Xavier, M. Dzaferagic, D. Collins, G. Comarela, M. Martinello, and M. Ruffini, "Machine learning-based early attack detection using open RAN intelligent controller," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2023, pp. 1856–1861.
- [24] S. Mayhoub et al., "A new sub-use case for signaling storm attack in open RAN and an ML-based detection approach," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2024, pp. 308–313.
- [25] R. Ma, H. Shi, H. Gao, H. Guan, M. Iqbal, and S. Mumtaz, "cFedDT: Cross-domain federated learning in digital twins for Metaverse consumer electronic products," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3167–3182, Feb. 2024.
- [26] "Amarisoft." Accessed: Dec. 4, 2024. [Online]. Available: <https://www.amarisoft.com/>
- [27] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session management for security systems in 5G Standalone network," *IEEE Access*, vol. 10, pp. 73421–73436, 2022.
- [28] "LTE MME documentation: Amarisoft tech academy." Accessed: Feb. 24, 2025. [Online]. Available: <https://tech-academy.amarisoft.com/Itemme.doc>
- [29] "Remote API: Amarisoft tech academy." Accessed: Mar. 6, 2025. [Online]. Available: <https://tech-academy.amarisoft.com/lteenb.doc#Remote-API-1>



George Xylouris (Member, IEEE) was born in Athens, in 1976. He received the bachelor's degree in physics from the University of Ioannina, and the master's degree in automation systems from the National Technical University of Athens, Greece. Since 2021, he has been serving as a Research Scientist and the Head of the Network Operations Center, NCSR "Demokritos." With a research portfolio that spans 6G Networks, software networks, edge-cloud and IoT continuum, and cybersecurity, he has authored over 130 scientific publications in

renowned international journals and conferences.



Athina Vekraki received the B.Sc. degree in informatics and telecommunications from the National and Kapodistrian University of Athens, where she is currently pursuing the M.Sc. degree in the field of data, information and knowledge management. She is a Research Associate with the Institute of Informatics and Telecommunications, NCSR "Demokritos."



Maria Christopoulou (Member, IEEE) received the B.Sc. degree in physics and the M.Sc. degree in radioelectrology and electronics from the National and Kapodistrian University of Athens in 2014 and 2016, respectively. She is currently pursuing the Ph.D. degree with the University of Peloponnese in the field of resource management in cellular telecommunication systems. She is a Research Associate with the Institute of Informatics and Telecommunications, NCSR "Demokritos."



Michail Alexandros Kourtis is a Researcher with the NCSR "Demokritos," working on NFV, SDN, 5G, and cybersecurity. He's been involved in several EU research projects and is the author of several publications in international journals and conferences (90+) in the respective fields. He has also collaborated as a contributor with ENISA on the "Threat Landscape for 5G Networks". He is currently the coordinator of four Horizon Europe projects in the domains of edge computing, cybersecurity certification, post-quantum cryptography, and governance.



Evangelos K. Markakis (Member, IEEE) is an Assistant Professor with the Hellenic Mediterranean University and a Principal Investigator with the PASIPHAE Lab, specializes in cybersecurity, IoT networks, and public safety communications. His research focuses on secure cyber-physical systems, edge networking, and privacy-enhancing security to protect IoT ecosystems against emerging threats. He has led numerous EU-funded projects, developing holistic security frameworks for critical infrastructures. Supporting the IEEE Public Safety Testbeds as the Co-Chair and serving as an Expert for ENISA, ETSI, and the European Defence Agency's CapTech, he advances AI-driven threat detection and secure communication protocols. With 120+ publications, his work supports the future of resilient, scalable, and secure networks.



Panagiotis Trakadas received the Dipl.-Ing. degree in electrical and computer engineering and the Ph.D. degree from the National Technical University of Athens. In the past, he was with the Hellenic Aerospace Industry as a Senior Engineer, on the design of military wireless telecommunications systems, and the Hellenic Authority for Communications Security and Privacy, where he held the position of the Director of the Division for the Assurance of Infrastructures and Telecommunications Services Privacy. He is currently an Associate Professor with the National and Kapodistrian University of Athens. He has been actively involved in many EU FP7 and H2020 research projects. He has published more than 130 papers in magazines, journals, and conference proceedings. His research interests include wireless and mobile communications, wireless sensor networking, network function virtualization, and cloud computing. He is a Reviewer of several journals, including IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE TRANSACTIONS ON ELECTROMAGNETIC COMPATIBILITY.