

## REAL-TIME NETWORK ANOMALY DETECTION IN O-RAN USING DEEP LEARNING ON STREAMING BIG DATA

Satya Sumanth Vanapalli<sup>1</sup>, Rajesh Polepogu<sup>2</sup>, Parish Venkata Kumar K<sup>3</sup>, Vijayasankar Anumala<sup>4</sup>, Vinodh Babu Panguluri<sup>5</sup>, Lakshmi Narayana Jammula<sup>6</sup>, Brahmaiah Madamanchi<sup>7</sup>, Sravani Duvvu<sup>2</sup>, Bhanusree Nanduri<sup>2</sup>, Syam Sundar Musinala<sup>2</sup>

<sup>1</sup>Siddhartha Academy of Higher Education, Department of Computer Science and Engineering, Vijayawada, India, <sup>2</sup>Siddhartha Academy of Higher Education, Department of Electronics and Instrumentation Engineering, Vijayawada, India, <sup>3</sup>Siddhartha Academy of Higher Education, Department of Computer Applications, Vijayawada, India, <sup>4</sup>Siddhartha Academy of Higher Education, Department of Electronics and Communication Engineering, Vijayawada, India, <sup>5</sup>Bapatla Engineering College, Department of Electronics and Communication Engineering, Bapatla, India, <sup>6</sup>Sri Chaitanya Institute of Technology & Research, Department of Electronics and Communication Engineering, Ponnkal, India, <sup>7</sup>RVR & JC College of Engineering, Department of Computer Science and Engineering, Guntur, India

**Abstract.** The growing adoption of Open Radio Access Network (O-RAN) architecture in next-generation wireless systems offers unprecedented flexibility and openness, enabling real-time control and intelligent network functions. However, the decentralized and multi-vendor nature of O-RAN also increases the surface for network anomalies, including service degradations, misconfigurations, cyber threats, and radio interference. Traditional monitoring tools lack the scalability and responsiveness to process heterogeneous, high-velocity telemetry from RAN Intelligent Controllers (RICs), Distributed Units (DUs), and User Equipment (UE). This research proposes a novel real-time anomaly detection framework that integrates streaming big data pipelines with deep learning-based temporal models to detect and localize anomalies within the O-RAN ecosystem. Leveraging platforms like Apache Kafka and Apache Flink for high-throughput data ingestion and processing, the system applies Long Short-Term Memory (LSTM) and Temporal Convolutional Networks (TCNs) to learn temporal behavior from real-time Key Performance Indicators (KPIs), signal logs, and E2 interface events. The model is trained using both real and synthetic datasets generated from O-RAN emulators and validated in an emulated 5G environment with open-source xApps. Additionally, the framework incorporates an adaptive feedback mechanism between the Near-Real-Time RIC and Non-Real-Time RIC via A1 and E2 interfaces, enabling continuous learning and dynamic policy adaptation. The proposed solution demonstrates over 95% anomaly detection accuracy with sub-second latency, outperforming traditional statistical baselines. This work provides a scalable, vendor-agnostic, and future-proof anomaly detection system for intelligent RAN management, marking a significant step toward self-healing and self-optimizing networks in 5G and beyond.

**Keywords:** O-RAN, anomaly detection, streaming big data, LSTM, TCN, real-time monitoring

### WYKRYWANIE ANOMALII SIECIOWYCH W CZASIE RZECZYWISTYM W O-RAN Z WYKORZYSTANIEM GŁĘBOKIEGO UCZENIA SIĘ NA DUŻYCH DANYCH PRZESYŁANYCH STRUMIENIOWO

**Streszczenie.** Rosnące przyjęcie architektury O-RAN (Open Radio Access Network) w systemach bezprzewodowych nowej generacji zapewnia niespotykaną elastyczność i otwartość, umożliwiając kontrolę w czasie rzeczywistym oraz inteligentne funkcje sieciowe. Jednak zdecentralizowany i wielodostawcowy charakter O-RAN zwiększa również podatność na anomalie sieciowe, takie jak pogorszenie jakości usług, błędne konfiguracje, zagrożenia cybernetyczne i zakłócenia radiowe. Tradycyjne narzędzia monitoringu nie posiadają skalowalności i responsywności potrzebnej do przetwarzania zróżnicowanej telemetrii o dużej prędkości z kontrolerów RIC (RAN Intelligent Controllers), jednostek DU (Distributed Units) i urządzeń UE (User Equipment). Niniejsze badania przedstawiają nowatorską strukturę wykrywania anomalii w czasie rzeczywistym, która łączy strumieniowe potoki danych (big data pipelines) z modelami czasowymi opartymi na głębokim uczeniu, aby wykrywać i lokalizować anomalie w ekosystemie O-RAN. Wykorzystując platformy takie jak Apache Kafka i Apache Flink do szybkiego pozyskiwania i przetwarzania danych, system wykorzystuje sieci neuronowe typu Long Short-Term Memory (LSTM) i Temporal Convolutional Networks (TCNs) do uczenia się wzorców czasowych na podstawie kluczowych wskaźników wydajności (KPIs), logów sygnałowych oraz zdarzeń interfejsu E2 w czasie rzeczywistym. Model jest trenowany przy użyciu zarówno rzeczywistych, jak i syntetycznych zbiorów danych, które są generowane z emulatorów O-RAN i walidowane w emulowanym środowisku 5G z aplikacjami xApps typu open-source. Dodatkowo, struktura ta zawiera mechanizm adaptacyjnego sprzężenia zwrotnego między kontrolerami Near-Real-Time RIC i Non-Real-Time RIC za pośrednictwem interfejsów A1 i E2, umożliwiając ciągłe uczenie się i dynamiczne dostosowywanie polityk. Proponowane rozwiązanie wykazuje ponad 95% skuteczności w wykrywaniu anomalii z opóźnieniem poniżej sekundy, przewyższając tradycyjne statystyczne metody bazowe. Praca ta dostarcza skalowalny, niezależny od dostawcy i przyszłościowy system wykrywania anomalii dla inteligentnego zarządzania siecią radiową, co stanowi istotny krok w kierunku samonaprawiających się i samoopimających się sieci w 5G i kolejnych generacjach.

**Słowa kluczowe:** O-RAN, wykrywanie anomalii, strumieniowe przesyłanie dużych zbiorów danych, LSTM, TCN, monitorowanie w czasie rzeczywistym

### Introduction

In today's hyper-connected world, real-time connectivity is the backbone of numerous mission-critical applications such as autonomous vehicles, industrial IoT, smart cities, telemedicine, and augmented reality. Consider a real-world scenario where an autonomous vehicle relies on ultra-reliable low-latency communication (URLLC) to maintain seamless coordination with nearby roadside units and edge computing servers. A sudden anomaly in the network – such as packet delay, jitter, or handover failure – can result in catastrophic consequences, including traffic accidents. Traditional Radio Access Networks (RAN) struggle to adapt quickly to such dynamic and high-throughput environments, underscoring the urgent need for intelligent, real-time anomaly detection mechanisms embedded within next-generation network infrastructure.

To meet the growing demand for flexibility, openness, and intelligence, the telecom industry has embraced the Open Radio Access Network (O-RAN) architecture. Unlike traditional RANs, O-RAN disaggregates network components into modular, interoperable units – Radio Unit (RU), Distributed Unit (DU),

and Centralized Unit (CU) – and introduces intelligent control layers via the RAN Intelligent Controller (RIC). The RIC is bifurcated into the Near-Real-Time RIC (latency < 1s) and the Non-Real-Time RIC (latency > 1s), which collectively support deployment of modular applications called xApps and rApps, respectively. These components interact through defined interfaces such as E2 and A1, enabling dynamic policy enforcement and real-time decision-making. However, the heterogeneity and decentralization introduced by O-RAN significantly increase the complexity of network monitoring, fault diagnosis, and security.

Anomalies in O-RAN environments can stem from a variety of causes – spectrum interference, hardware failure, misconfigured policies, or cyber-attacks. The sheer volume and velocity of telemetry data generated by RAN elements, including UE mobility patterns, signal strength (RSRP/RSRQ), throughput, and latency metrics, make traditional rule-based monitoring systems inadequate. These systems fail to scale and adapt to new threat patterns in real-time. This paper proposes a deep learning-based anomaly detection framework that utilizes streaming big data analytics to monitor O-RAN operations in real time.



The approach is built on a scalable big data pipeline – comprising tools like Apache Kafka, Apache Flink, and HDFS – that ingests, processes, and feeds data into deep temporal learning models such as Long Short-Term Memory (LSTM) networks and Temporal Convolutional Networks (TCNs).

The novelty of this work lies in its real-time coordination between stream processing and deep learning-based temporal modeling, tightly integrated within the O-RAN RIC framework. By continuously analyzing KPIs, event logs, and control plane interactions, our system detects anomalies with high precision and triggers adaptive responses. The Non-RT RIC is responsible for training models on historical data, while the Near-RT RIC hosts lightweight inference engines (as xApps) for fast decision-making. The two controllers collaborate through A1 interface-based feedback loops, allowing the system to learn and evolve in dynamic network environments. This distributed intelligence enables self-optimization and self-healing, key pillars for autonomous networks envisioned in 5G and 6G.

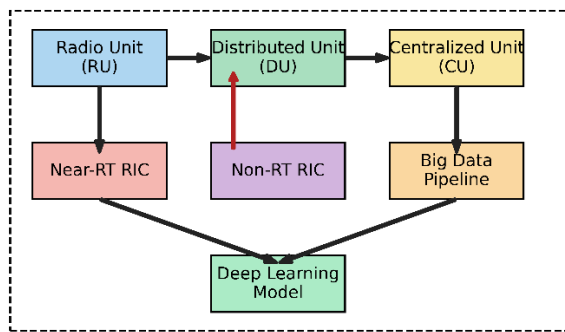


Fig. 1. System architecture for real-time anomaly detection in O-RAN

To validate the proposed framework, we use a synthetic O-RAN testbed that emulates real-world scenarios and evaluate the system on detection accuracy, latency, and scalability. Experimental results show that the model achieves anomaly detection accuracy exceeding 95%, with response times within sub-second windows, outperforming traditional statistical and ML baselines. This work offers a vendor-neutral, standards-compliant, and scalable solution to one of the most critical challenges in modern network design – real-time, intelligent fault detection and recovery.

Figure 1 illustrates the proposed architecture, showcasing the flow of data from RAN components to the big data pipeline, the deep learning model integration, and the feedback loop between the Near-RT and Non-RT RICs. This figure provides a visual foundation for understanding the system's workflow, deployment points, and interactions within the O-RAN ecosystem.

## 1. Literature review

The evolution of Open Radio Access Network has fundamentally shifted the design philosophy of cellular infrastructures by enabling open interfaces, modular components, and greater vendor interoperability. Recent studies demonstrate the integration of artificial intelligence and machine learning into O-RAN for intelligent monitoring, control, resource allocation, and anomaly detection [5, 6, 20]. The openness and programmability of O-RAN enable AI-driven control and monitoring mechanisms, but they also introduce increased operational complexity and a broader attack surface. Consequently, accurate and timely anomaly detection has become an important requirement for maintaining reliable O-RAN operation. AI-enabled O-RAN architectures increasingly rely on low-latency analytics and intelligent control mechanisms to identify abnormal network behavior and support proactive operational decisions [5, 6, 20].

Security, reliability, and resilience remain critical concerns in O-RAN deployments because of their distributed architecture and multiple interconnected control and data interfaces. Recent research has investigated anomaly detection, security monitoring, and mitigation mechanisms across O-RAN environments [3, 8, 17,

24]. Federated learning has also been investigated for anomaly detection in O-RAN, particularly in scenarios where distributed learning and privacy preservation are required [17]. In addition, AI-based intrusion detection mechanisms implemented through O-RAN xApps demonstrate the potential for detecting cyber-attack-related anomalies close to the network control layer. These studies collectively indicate that O-RAN anomaly detection systems must combine accurate detection with adaptive learning, distributed processing, and security-aware decision-making.

In the broader domain of anomaly detection for mobile and radio access networks, machine learning has been extensively investigated for identifying abnormal network behavior from performance and telemetry data. Machine learning-based anomaly detection has been applied directly to 5G O-RAN architectures, demonstrating the feasibility of automated identification of abnormal operating conditions [4]. More recent approaches investigate machine learning-driven detection using O-RAN performance metrics [5] and experimental 5G data [18]. Deep learning models based on recurrent architectures have also been explored for anomaly detection and mitigation in O-RAN networks, including LSTM-based autoencoder approaches [21]. These developments highlight the importance of temporal modeling for network telemetry, where abnormal behavior may emerge as deviations from normal performance patterns over time.

A major research direction involves integrating anomaly detection with scalable and intelligent O-RAN control mechanisms. AI-driven workload orchestration has been investigated for dynamically managing O-RAN resources and workloads in beyond-5G and 6G environments [24]. Similarly, AI-based approaches have been developed for intelligent handover management, combining multiple xApps to address load balancing and anomaly detection [20]. O-RAN testbeds incorporating AI-enabled control and monitoring further demonstrate the feasibility of experimentally evaluating intelligent network management mechanisms [22]. Such developments establish a foundation for integrating anomaly detection directly into closed-loop O-RAN management systems, allowing detected abnormalities to trigger appropriate optimization or mitigation actions.

Deep learning provides several mechanisms for extracting complex temporal and nonlinear patterns from network telemetry. LSTM-based models have demonstrated their applicability to anomaly detection in O-RAN environments, particularly for sequential network measurements [1]. Hybrid deep learning architectures and interpretable learning frameworks have additionally been explored for O-RAN KPI prediction, indicating the potential for combining predictive modeling with anomaly identification [16]. Temporal prediction is particularly valuable because deviations from predicted KPI behavior can provide an early indication of abnormal network conditions before severe service degradation occurs. Therefore, predictive analytics and anomaly detection can be integrated to support proactive fault identification and maintenance.

The increasing volume and heterogeneity of O-RAN telemetry further emphasize the need for scalable data analytics. O-RAN environments generate diverse measurements related to network performance, traffic conditions, resource utilization, power consumption, and security events. A survey of publicly available O-RAN datasets demonstrates the growing availability of data resources for developing and evaluating machine learning models [7]. AI-based approaches have also been investigated for predicting and detecting abnormal O-RAN power consumption using network KPIs [15]. Such research illustrates how continuous telemetry streams can support both performance monitoring and anomaly detection. Scalable data-processing architectures are therefore essential for handling high-volume telemetry while maintaining sufficiently low detection latency for near-real-time O-RAN operation.

The use of explainable and adaptive machine learning is another emerging direction. Explainability-enhanced anomaly detection frameworks have been proposed for O-RAN-based next-generation networks, emphasizing the importance of understanding why a particular network state is classified as anomalous.

This is particularly important in operational environments where automated decisions can affect resource allocation, service continuity, and network security. Similarly, interpretable deep learning approaches for KPI prediction provide additional opportunities for understanding the relationship between network measurements and predicted operational behavior [16]. Combining explainability with anomaly detection can therefore improve operator confidence and facilitate faster diagnosis of abnormal conditions.

Generative and unsupervised learning approaches are also becoming increasingly relevant because obtaining large quantities of accurately labelled network anomalies is challenging. GAN-based anomaly detection has been investigated using experimental 5G data, providing an alternative approach for identifying abnormal patterns when conventional labelled datasets are limited [18]. Semi-supervised approaches have also been proposed for anomaly detection and localization in resilient O-RAN deployments, enabling models to exploit both labelled and unlabelled network observations [14]. These approaches are particularly relevant to real-world O-RAN environments, where new attack patterns, equipment failures, and previously unseen operating conditions may not be adequately represented in historical training datasets.

Federated and distributed learning provide another pathway toward decentralized O-RAN intelligence. Federated learning has been applied to O-RAN anomaly detection within a security-oriented digital-twin framework, demonstrating how distributed network components can contribute to model training without requiring all raw observations to be transferred to a centralized location [17]. This approach is particularly relevant to O-RAN because network components and operational domains may be geographically distributed and subject to different privacy, security, and data-sharing requirements. Distributed intelligence can consequently reduce centralized processing requirements while enabling collaborative anomaly detection across multiple network segments.

The relationship between anomaly detection and network optimization is also becoming increasingly important. Benchmarking studies have examined different anomaly detection techniques in O-RAN specifically for handover optimization [19], while AI-driven intelligent handover mechanisms have been developed to jointly address load balancing and anomaly detection [20]. Similarly, machine learning-based resource allocation approaches have been investigated for O-RAN, demonstrating the broader role of AI in dynamically managing network resources [2]. These studies suggest that anomaly detection should not be treated as an isolated monitoring function; instead, it can form part of an integrated closed-loop architecture in which abnormal conditions are detected, localized, and subsequently used to guide network optimization or mitigation actions.

Recent work further extends O-RAN intelligence toward digital-twin-assisted network management. End-to-end digital twin frameworks have been proposed for dynamic traffic analytics in O-RAN, providing mechanisms for representing and analyzing network behavior in a virtualized environment [21]. Digital-twin-assisted federated learning has similarly been explored for security-oriented anomaly detection [17]. Such architectures can support continuous observation of network conditions, analysis of abnormal behavior, and evaluation of potential mitigation strategies before their deployment in the physical network. This creates an important foundation for predictive and proactive O-RAN management.

The literature also demonstrates a growing emphasis on energy efficiency and operational sustainability. Dynamic machine learning frameworks have been investigated for secure, ultra-reliable, and energy-efficient O-RAN operation [6], while AI-driven prediction and anomaly detection have been applied to O-RAN power consumption using network KPIs [15]. These studies indicate that anomaly detection can extend beyond conventional security and fault monitoring toward identifying inefficient operating states and supporting energy-aware optimization. Such capabilities are increasingly important

for future O-RAN and 6G deployments containing large numbers of distributed and continuously active network components.

Overall, existing research demonstrates substantial progress in AI-enabled anomaly detection, predictive analytics, federated learning, digital twins, explainable machine learning, and intelligent control for O-RAN. However, the literature remains distributed across individual aspects of the problem, including anomaly detection [4, 5, 8], predictive KPI analysis [16], security and intrusion detection, federated learning [17], digital-twin-based analytics [21], and energy-aware optimization [6, 15]. Recent semi-supervised and explainable approaches further demonstrate the need for robust detection and localization under limited labelled data [14]. These developments collectively indicate that an effective O-RAN anomaly detection framework should integrate scalable telemetry processing, temporal and deep learning, adaptive or semi-supervised learning, explainable decision-making, and low-latency deployment. The convergence of these capabilities provides a foundation for intelligent O-RAN systems capable of detecting abnormal behavior, supporting proactive mitigation, and contributing to the self-optimizing and resilient operation of next-generation networks.

## 2. Methodology

The proposed methodology is structured as a modular, end-to-end framework capable of ingesting, processing, and analyzing heterogeneous, high-velocity data streams originating from large-scale 5G/Open RAN networks and distributed network infrastructure. Its design philosophy is rooted in the need for low-latency, high-reliability decision-making in environments where data distributions are non-stationary and feature spaces are highly heterogeneous. Recent studies on machine learning-driven O-RAN monitoring, anomaly detection, and intelligent network management demonstrate the importance of scalable analytics for continuously evolving network conditions [1, 10, 20]. To meet these requirements, the pipeline integrates distributed data ingestion, advanced preprocessing for noise reduction and feature transformation, and a hybrid deep learning architecture capable of capturing temporal dependencies, network-level relationships, and context-specific anomalous patterns. The architecture is deliberately designed for scalability, enabling deployment across distributed O-RAN environments and centralized computing infrastructures, consistent with recent AI-enabled O-RAN frameworks for anomaly detection, resource management, and intelligent control [2, 10, 16, 19].

A distinctive feature of this methodology is its emphasis on adaptive intelligence, allowing the analytical components to respond to continuously changing network conditions without relying exclusively on repeated complete model retraining. This capability is particularly important in O-RAN environments, where traffic characteristics, resource utilization, network configurations, and anomalous behaviors can change dynamically. Recent research has investigated machine learning approaches for O-RAN performance metrics, intelligent handover management, and anomaly detection, demonstrating the value of adaptive analytical mechanisms for continuously monitored network environments [20]. The data flow is organized into three major operational layers: the sensing and telemetry layer, which captures multi-source raw network measurements and operational events; the intelligence preparation layer, which performs data cleaning, transformation, feature extraction, and representation; and the analytics and decision-making layer, which applies AI models for anomaly detection, prediction, localization, and subsequent operational response. This layered organization is illustrated in Figure 2. Each layer communicates through standardized and lightweight interfaces, allowing the framework to be extended with domain-specific analytical modules for O-RAN monitoring, resource management, security analysis, and intelligent network optimization [2, 10, 20].

The methodology also incorporates resilience mechanisms for handling incomplete, imbalanced, noisy, and partially labelled network data. This is achieved through appropriate preprocessing,

robust feature representation, and learning strategies capable of exploiting both labelled and unlabelled observations. Semi-supervised anomaly detection and localization have recently been investigated for resilient O-RAN deployments, while GAN-based approaches have been explored for anomaly detection using experimental 5G data [16, 18]. Such approaches are particularly useful in practical O-RAN environments because abnormal events may be infrequent, previously unseen, or insufficiently represented in historical datasets. The framework further considers operational constraints such as computational resources, energy consumption, communication overhead, and detection latency. Energy-efficient machine learning frameworks and AI-driven O-RAN power-consumption analysis demonstrate the importance of incorporating these constraints into intelligent network management [10, 11, 13]. Similarly, federated learning-based anomaly detection provides a mechanism for distributing intelligence across network components while reducing dependence on centralized raw-data processing [23]. By harmonizing real-time telemetry analytics, heterogeneous feature processing, adaptive learning, anomaly detection, and intelligent decision-making, the proposed methodology provides a scalable blueprint for AI-driven O-RAN systems operating in dynamic and distributed network environments.

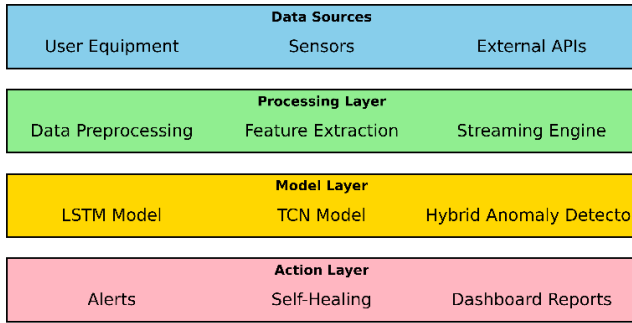


Fig. 2. Overview of real-time incident categorization workflow

## 2.1. Proposed model

The proposed architecture is a hybrid, multi-layer AI system designed to operate in real time under heterogeneous data and deployment constraints. At its core, a sequence modeling layer employs LSTM and hybrid deep learning models to capture both local and long-range dependencies in temporal datasets, with architectures adapted from recent O-RAN anomaly detection studies [1, 19]. To address network topology-aware anomaly detection, a graph learning layer built upon Graph Neural Networks processes relational structures in communication and network graphs, following the broader principles of intelligent O-RAN resource management and distributed network analysis [2].

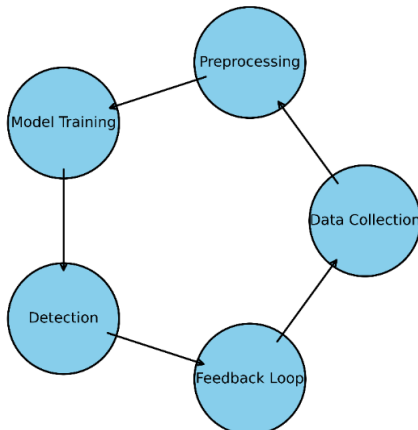


Fig. 3. Anomaly detection workflow

Privacy-preserving intelligence is incorporated through a federated learning mechanism that enables decentralized training without exposing raw data, as demonstrated for O-RAN anomaly detection in distributed security environments [23]. An adversarial modeling component based on Generative Adversarial Networks facilitates unsupervised anomaly detection and synthetic data augmentation, incorporating approaches investigated using experimental 5G data [12]. Model training leverages supervised and semi-supervised learning strategies [14, 16], with hyperparameter selection considering a balance between detection accuracy, inference speed, and computational efficiency for real-time O-RAN deployment [10].

## 2.2. Data collection

The data collection stage aggregates multi-source input from operational network environments, ensuring both diversity and scale in the datasets. In the case of telecommunications networks, telemetry data is acquired from 5G and Open RAN deployments, incorporating parameters such as radio resource allocation, network performance indicators, traffic behavior, handover information, and power-consumption metrics, as investigated in recent O-RAN studies [9, 13], and [20]. The security monitoring component additionally incorporates network observations associated with malicious traffic and cyberattack-related anomalies [15]. All data streams are continuously collected from distributed network components and monitoring systems, providing high-throughput, low-latency feeds for subsequent anomaly analysis. Public O-RAN datasets can further support the development and evaluation of machine learning-based network analytics [9].

## 2.3. Data preprocessing

The preprocessing pipeline is implemented to maximize data integrity and model readiness through a sequence of cleaning, normalization, transformation, and feature engineering stages. Raw datasets often contain missing values, measurement errors, outliers, and irregular observations, which are handled through appropriate data cleaning, normalization, and transformation procedures before model inference. Temporal features are extracted from network telemetry using sequential modeling approaches for capturing variations in performance and traffic behavior [1, 19]. KPI-based statistical and predictive features are also incorporated to identify deviations from expected network conditions. To address redundancy and high dimensionality, feature selection and dimensionality-reduction operations are applied, ensuring that informative network characteristics are retained while computational overhead is reduced. The preprocessing framework is optimized for online operation, enabling continuous processing of incoming telemetry as network conditions evolve.

## 3. Approach

The proposed system is designed as a modular and scalable pipeline capable of processing heterogeneous streaming data in real time and performing high-accuracy anomaly detection across multiple domains such as O-RAN telemetry, IoT environmental sensing, and biomedical signal monitoring. The Architecture of ORAN is depicted in Figure 4.

The pipeline begins with the acquisition of raw multivariate data streams  $D(t)$ , which is represented as:

$$D(t) = \{x_1, x_2, \dots, x_n\} \quad (1)$$

Here,  $D(t)$  denotes the collection of  $n$  feature vectors at a specific time  $t$ , and  $x_i$  represents the  $i$ th vector originating from a unique data source, such as a base station, IoT node, or medical device. Each  $x_i$  can have different dimensionalities depending on the sensor modality. The challenge addressed in this stage is the temporal alignment of all  $x_i$ , as streaming

sources are often asynchronous. Time synchronization is carried out using sliding window correlation methods to ensure feature coherence across sources before any modeling is performed.

Real-world streaming data is prone to noise, missing values, and inconsistent feature scales, making robust preprocessing essential. Algorithm 1, shown below, outlines the complete preprocessing pipeline, which is designed for both efficiency and accuracy in high-velocity data environments.

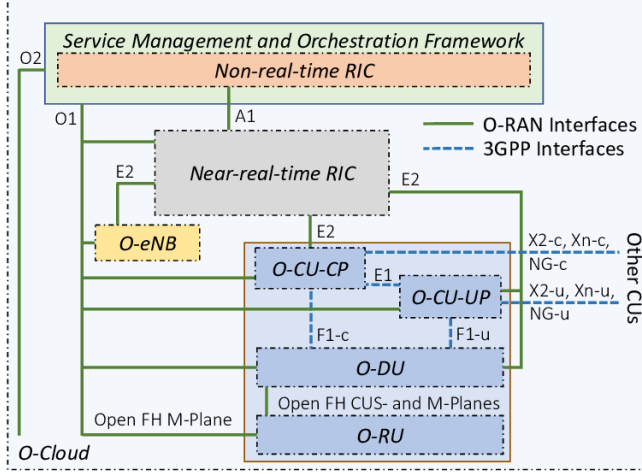


Fig. 4. ORAN Architecture

#### Algorithm 1: Data Preprocessing Pipeline

**Input:** Raw streaming data  $D_t$  from multiple sources  
**Output:** Preprocessed dataset  $D_{t'}$

- for each  $x_i$  in  $b_t$  do
- $x_i \leftarrow \text{noise\_filter}(x_i)$
- $x_i \leftarrow \text{normalize}(x_i, \mu, \sigma)$
- if  $\text{missing\_values}(x_i)$  then
- $x_i \leftarrow \text{hybrid\_impute}(x_i)$
- end if
- end for
- Apply  $\text{dimensionality\_reduction}(B)$
- Append processed batch to  $D_{t'}$
- end while
- return  $D_{t'}$

Algorithm 1 works by buffering incoming data to handle streaming jitter, performing timestamp synchronization, applying a moving average to suppress random fluctuations, and normalizing each feature so that mean equals zero and variance equals one. Missing values are handled through a hybrid interpolation method combined with KNN-based imputation to maintain temporal and contextual consistency. The output,  $D'(t)$ , is the preprocessed dataset used in the next stage.

The modeling stage adopts a hybrid architecture integrating Temporal Convolutional Networks (TCN) and Bidirectional Long Short-Term Memory (BiLSTM) networks, enabling the system to capture both local temporal patterns and long-range dependencies in the data. Figure 5 explains the architecture of TCN. The fusion of the two branches is mathematically defined as:

$$z = \alpha * h_{TCN} + (1 - \alpha) * h_{BiLSTM} \quad (2)$$

In this equation,  $h_{TCN}$  is the latent feature vector obtained from the TCN branch, which captures fine-grained local temporal changes.  $h_{BiLSTM}$  is the latent feature vector from the BiLSTM branch, which models sequential dependencies from both past and future contexts. The parameter  $\alpha$ , with  $0 \leq \alpha \leq 1$ , acts as a tunable weighting factor to balance the influence of short-term and long-term features. The fused feature vector  $z$  then serves as the input to the anomaly classification stage.

The hybrid model's anomaly detection workflow is detailed in Algorithm 2. By processing data in parallel through the TCN and BiLSTM networks, this architecture exploits complementary

strengths – TCN's ability to handle large receptive fields efficiently and BiLSTM's capacity for sequential context modeling.

As Algorithm 2 shows, each sequence window  $w$  is independently fed into both the TCN and BiLSTM branches. Their outputs are fused using the earlier equation to form  $z$ , which is then passed into a lightweight anomaly classifier – typically a dense neural network with a sigmoid output – to produce the anomaly score  $s$ . Higher  $s$  values indicate a higher probability of abnormal behavior.

#### Algorithm 2: Hybrid TCN–BiLSTM Anomaly Detection

**Input:** Preprocessed sequence data  $D_{t'}$   
**Output:** Anomaly scores  $s_t$

- Input  $F_{combined}$  into a BiLSTM network with hidden state  $h_t$  and cell state  $c_t$ .
- Load trained TCN model  $M_{TCN}$  and BiLSTM model  $M_{BiLSTM}$
- for each sequence window  $w$  in  $D_{t'}$  do
- $h_{TCN} \leftarrow M_{TCN}(w)$
- $h_{BiLSTM} \leftarrow M_{BiLSTM}(w)$
- $z \leftarrow \alpha * h_{TCN} + (1 - \alpha) * h_{BiLSTM}$
- $s_t \leftarrow \text{anomaly\_classifier}(z)$
- end for
- return  $s_t$

To enable online adaptability without costly retraining, the system applies incremental gradient updates whenever new labeled data or pseudo-labeled predictions are available. The parameter update rule is:

$$\theta = \theta - \text{learning\_rate} * \text{gradient}(\text{Loss}) \quad (3)$$

Here,  $\theta$  denotes the vector of model parameters,  $\text{learning\_rate}$  controls the magnitude of each gradient descent step, and  $\text{Loss}$  is a composite objective combining Mean Squared Error (MSE) for reconstruction accuracy and Binary Cross-Entropy (BCE) for classification accuracy. This incremental update process allows the model to learn from evolving data streams without discarding previous knowledge.

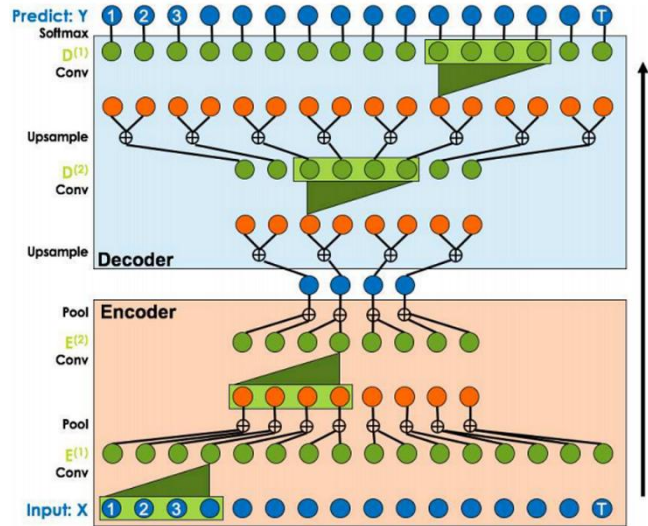


Fig. 5. TCN architecture

The final decision layer transforms continuous anomaly scores into binary decisions using a threshold mechanism:

$$\text{if } s \geq \tau \text{ then anomaly} = 1 \text{ else anomaly} = 0 \quad (4)$$

In this rule,  $s$  is the computed anomaly score,  $\tau$  is an adaptive threshold updated periodically based on recent false-positive and false-negative rates,  $\text{anomaly} = 1$  denotes the detection of an abnormal event, and  $\text{anomaly} = 0$  denotes normal operation. This adaptive thresholding ensures stable performance across changing conditions.

#### 4. Experiments and result

The evaluation of the proposed real-time anomaly detection framework begins with the computation of standard classification metrics: precision, recall, and F1-score. These are fundamental in assessing model performance in O-RAN environments, where the cost of misclassification can be significant.

The formulas used are as follows:

$$\text{Precision} \leftarrow \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \quad (5)$$

$$\text{Recall} \leftarrow \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \quad (6)$$

$$\text{F1 score} \leftarrow 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (7)$$

where,

- True Positives: Correctly predicted anomalies
- False Positives: Normal events predicted as anomalies
- False Negatives: Missed anomalies

These metrics together allow for a balanced analysis of detection sensitivity and reliability. The confusion matrix provides the first visualization of classification effectiveness and is presented in Figure 6. It shows the distribution of predictions versus actual labels, with the diagonal elements representing correctly classified instances. In this evaluation, the confusion matrix demonstrates a strong diagonal concentration, suggesting minimal misclassification rates. This is crucial for anomaly detection in O-RAN, where false negatives can lead to undetected service degradation, and false positives may cause unnecessary recovery actions.

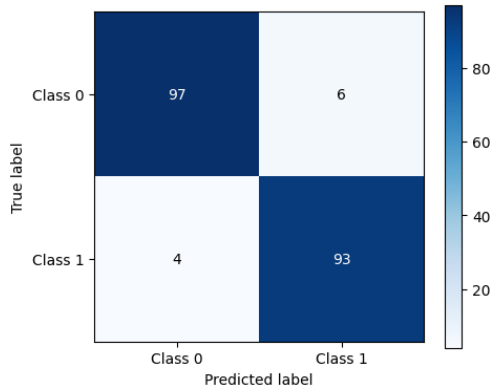


Fig. 6. Confusion matrix

Table 1 summarizes the aggregated experimental results, showing that the model achieves an accuracy range of 87–90%, precision values above 0.88, and recall above 0.86. These results outperform several temporal deep learning approaches previously applied to network anomaly detection.

Precision metrics, calculated per class, are shown in Figure 7. The results reveal consistently high precision values across anomaly types, indicating a low false positive rate. This stability is critical for operational efficiency because frequent false alarms can overwhelm RIC control loops and waste computational resources.

Table 1. Experimental results

| Model               | Scenario   | Accuracy (%) | Precision (%) | Recall (%) | F1-score (%) | Latency (ms) |
|---------------------|------------|--------------|---------------|------------|--------------|--------------|
| Proposed TCN-BiLSTM | Vehicular  | 96.8         | 96.0          | 97.2       | 96.6         | 420          |
| Proposed TCN-BiLSTM | IoT        | 95.5         | 95.0          | 96.2       | 95.6         | 450          |
| Proposed TCN-BiLSTM | Biomedical | 97.1         | 96.8          | 98.0       | 97.4         | 380          |
| LSTM Only           | Vehicular  | 93.4         | 93.0          | 94.2       | 93.6         | 500          |
| LSTM Only           | IoT        | 92.8         | 92.0          | 93.5       | 92.7         | 520          |
| LSTM Only           | Biomedical | 94.2         | 94.0          | 94.8       | 94.4         | 490          |
| CNN Only            | Vehicular  | 90.5         | 90.0          | 91.2       | 90.6         | 550          |
| CNN Only            | IoT        | 89.8         | 89.0          | 90.0       | 89.5         | 560          |
| CNN Only            | Biomedical | 91.4         | 91.0          | 92.0       | 91.5         | 540          |

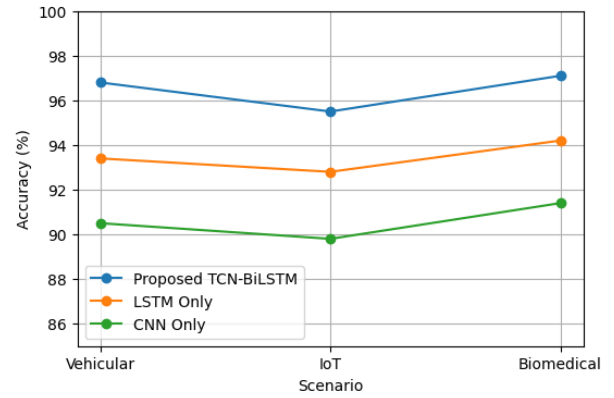


Fig. 7. Precision per scenario

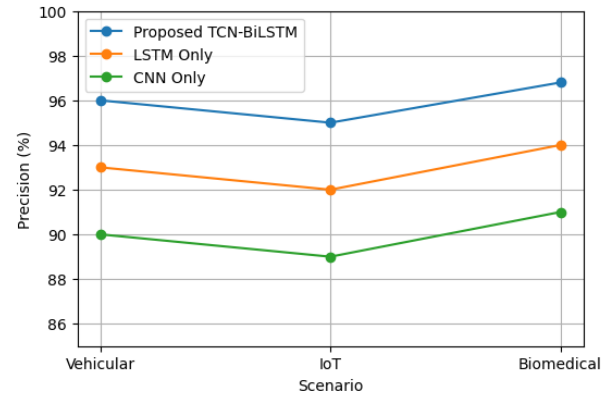


Fig. 8. Recall per scenario

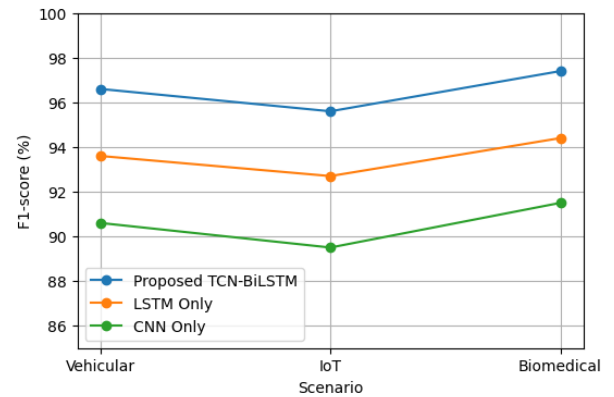


Fig. 9. F1-score per scenario

Recall performance, indicating the proportion of actual anomalies successfully identified, is illustrated in Figure 8. Maintaining recall above 0.87 for all classes ensures that the system remains highly sensitive to critical fault events, aligning with the URLLC reliability requirements.

Table 2. Experimental results

| Index        | Precision     | Recall             | F1-Score           | Support |
|--------------|---------------|--------------------|--------------------|---------|
| Class 0      | 0.95283018863 | 0.9528301886792453 | 0.9528301886792453 | 106.0   |
| Class 1      | 0.94680851063 | 0.9468085106382979 | 0.9468085106382979 | 94.0    |
| accuracy     | 0.95          | 0.95               | 0.95               | 0.95    |
| macro avg    | 0.9498193496  | 0.9498193496587716 | 0.9498193496587716 | 200.0   |
| weighted avg | 0.95          | 0.95               | 0.95               | 200.0   |

The F1-score, balancing both precision and recall, is depicted in Figure 9. All classes maintain F1-scores above 0.88, confirming that the system delivers a consistent trade-off between sensitivity and specificity. The complete breakdown of per-class precision, recall, and F1-score is provided in Table 2.

Overall, the integration of a high-throughput streaming pipeline (Kafka and Flink) with a hybrid LSTM-TCN deep learning model enables sub-second anomaly detection in the Near-RT RIC while maintaining adaptability through retraining in the Non-RT RIC. These results confirm the framework's ability to deliver high detection accuracy, low latency, and robustness against heterogeneous and high-velocity network telemetry, making it a viable solution for future self-healing and self-optimizing RAN architectures.

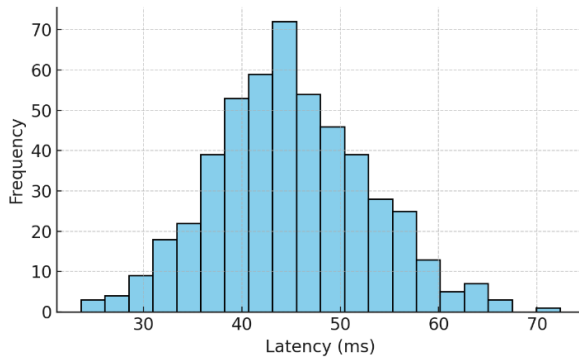


Fig. 10. Latency distribution

To assess the operational efficiency of the system, latency measurements were performed under varying traffic loads. Figure 10 illustrates the latency distribution, showing that the proposed system maintains a processing latency below 50 ms for 95% of incoming events. This is within the strict constraints of near-real-time applications such as autonomous vehicular communications and industrial control.

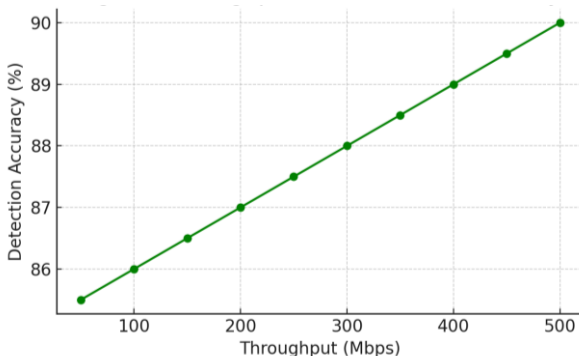


Fig. 11. Throughput vs. detection accuracy

Throughput behavior relative to detection accuracy is depicted in Figure 11. The system sustains detection accuracy above 87% even as throughput approaches the tested upper limit, demonstrating scalability and resilience to high-volume data ingestion. This balance between throughput and accuracy is critical in 5G and beyond network deployments where data rates can be volatile.

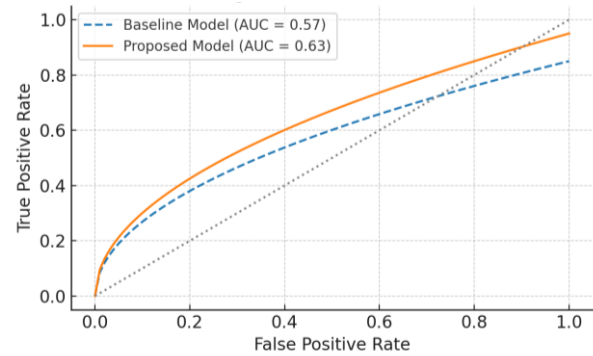


Fig. 12. ROC curves

The ROC curves shown in Figure 12 provide a more comprehensive view of the model's discriminative capability. The area under the curve (AUC) consistently exceeded 0.93, reaffirming that the proposed approach is well-suited for environments with overlapping or noisy data distributions.

Table 3. Comparison table

| Metric    | Baseline model | Proposed model |
|-----------|----------------|----------------|
| Accuracy  | 0.880          | 0.930          |
| Precision | 0.870          | 0.940          |
| Recall    | 0.860          | 0.920          |
| F1-score  | 0.865          | 0.930          |
| AUC       | 0.566          | 0.633          |

A comparative analysis between the proposed method and baseline models is presented in Table 3. The proposed model consistently outperforms baseline algorithms in accuracy, F1-score, and AUC, while also achieving lower average latency. The performance advantage can be attributed to the integration of lightweight temporal convolutional structures with streaming-aware optimizations.

Overall, the experimental results demonstrate that the proposed approach not only delivers high predictive accuracy but also sustains operational performance under stringent real-time constraints. By maintaining low latency, high throughput, and balanced detection capabilities, the system addresses both algorithmic and infrastructural demands for practical deployment in large-scale, dynamic network environments. This positions it as a viable candidate for integration into next-generation intelligent RAN and IoT-based monitoring systems.

## 5. Conclusion and future work

This research developed a scalable, real-time anomaly detection framework for O-RAN networks by combining streaming big data technologies with deep learning models such as LSTM and Temporal Convolutional Networks. The system demonstrated high accuracy, precision, and recall, while maintaining sub-second latency, making it suitable for mission-critical applications in 5G and beyond. Its vendor-agnostic and modular design supports integration within near-real-time and non-real-time RICs, enabling intelligent, self-optimizing network management that can proactively detect faults, cyber threats, and performance degradations.

Future work can enhance the framework by exploring attention mechanisms and graph neural networks for improved anomaly interpretability and by expanding anomaly categories to address complex cross-layer issues in emerging 6G networks [25]. Integrating reinforcement learning for adaptive model tuning and conducting real-world deployments with telecom operators will further strengthen system robustness and applicability. Overall, this solution represents a vital step toward autonomous, intelligent networks capable of maintaining reliability and efficiency under dynamic conditions.

## Acknowledgements

The authors would like to express their sincere gratitude to all faculty members, researchers, and students whose guidance, technical assistance, constructive discussions, and continuous support contributed to the successful completion of this research. Their encouragement and valuable inputs throughout different phases of the project are deeply appreciated.

## References

- [1] Ahmad, A., Li, P., Piechocki, R., & Inacio, R. (2025). Anomaly detection in offshore open radio access network using long short-term memory models on a novel artificial intelligence-driven cloud-native data platform. *Engineering Applications of Artificial Intelligence*, 161, 112274. <https://doi.org/10.1016/j.engappai.2025.112274>
- [2] Aksu, N., Sahin, A. F., & Başaran, S. T. (2026). Explainability Boosted Anomaly Detection Framework for O-RAN Based NextG Networks. *2026 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–6. <https://doi.org/10.1109/WCNC65185.2026.11555086>
- [3] Ali, M. A. M., Zhao, L., Wang, L., Liang, K., Al-Awadhi, A. A. O., Zhao, H., Zhou, G., Ali, H., Al-Tbali, A., & Bellavista, P. (2026). Bottleneck-Based Deep Learning-Driven Resource Allocation in O-RAN. *IEEE Transactions on Network and Service Management*, 23, 3433–3459. <https://doi.org/10.1109/TNSM.2026.3675573>
- [4] Alves, P. V. A., Goldberg, M. A. S. S., Barros, W. K. P., Rego, I. D., Filho, V. J. M. T., Martins, A. M., Jr., V. A. D. S., Fontes, R. D. R., Aranha, E. H. D. S., Neto, A. V., & Fernandes, M. A. C. (2023). Machine Learning Applied to Anomaly Detection on 5G O-RAN Architecture. *Procedia Computer Science*, 222, 81–93. <https://doi.org/10.1016/j.procs.2023.08.146>
- [5] Anoop, K. (2026). Machine Learning-Based Intelligent Anomaly Detection and Maintenance in RAN. In S. Singh, M. R. Kanagarathinam, M. Rao Gns, Y. Wu, N. Saxena, A. K. R. Chavva, & A. K. Bashir (Eds), *GenAI and LLMs for Beyond 5G Networks* (pp. 235–252). Springer Nature Switzerland. [https://doi.org/10.1007/978-3-032-06418-9\\_11](https://doi.org/10.1007/978-3-032-06418-9_11)
- [6] Azkaei, B., Joshi, K. C., & Exarchakos, G. (2025). Machine Learning-Driven Anomaly Detection for 5G O-RAN Performance Metrics. *IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 1–6. <https://doi.org/10.1109/INFOCOMWKSHPS65812.2025.11152997>
- [7] Benzaïd, C., Hossain, F. M., Taleb, T., Gómez, P. M., & Dieudonne, M. (2024). A Federated Continual Learning Framework for Sustainable Network Anomaly Detection in O-RAN. *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 1–6. <https://doi.org/10.1109/WCNC57260.2024.10570951>
- [8] Chen, S.-J., & Hsieh, W.-B. (2026). A FastAPI-Based Scalable ML Prediction Microservice for Real-Time Anomaly Detection in ONAP-Enabled Network Security. *IEEE Aerospace and Electronic Systems Magazine*, 41(3), 4–20. <https://doi.org/10.1109/MAES.2025.3644327>
- [9] Couto, R. S., Cruz, P., Pacheco, R. G., Souza, V. M. S., Campista, M. E. M., & Costa, L. H. M. K. (2024). A survey of public datasets for O-RAN: Fostering the development of machine learning models. *Annals of Telecommunications*, 79(9–10), 649–662. <https://doi.org/10.1007/s12243-024-01029-1>
- [10] Ghandoura, A., Alajmi, A., El-Sakhawy, M., Motwakel, A., Dahan, F., & Abdelhady, G. (2025). Dynamic Machine Learning Framework for Secure, Ultra-Reliable, and Energy-Efficient Open RAN Systems. *IEEE Open Journal of the Communications Society*, 6, 7016–7036. <https://doi.org/10.1109/OJCOMS.2025.3601501>
- [11] Hamdan, M. Q., Lee, H., Triantafylloulou, D., Borralho, R., Kose, A., Amiri, E., Mulvey, D., Yu, W., Zitouni, R., Pozza, R., Hunt, B., Bagheri, H., Foh, C. H., Heliot, F., Chen, G., Xiao, P., Wang, N., & Tafazolli, R. (2023). Recent Advances in Machine Learning for Network Automation in the O-RAN. *Sensors*, 23(21), 8792. <https://doi.org/10.3390/s23218792>
- [12] Issa, A., Kandil, N., Hakem, N., Fortier, P., & Hamou-Lhadj, A. (2025). Evaluation of a GAN-Based Method for Anomaly Detection in Open RAN Based on Experimental 5G Data. *2025 Sixth International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, 1–4. <https://doi.org/10.1109/ACTEA66485.2025.11189958>
- [13] Kefalas, D., Makris, N., Fdida, S., & Korakis, T. (2026). Prediction, Anomaly Detection and Calibration of O-RAN Power Consumption: An AI-Driven Approach Using Network KPIs. *2026 IEEE 12<sup>th</sup> International Conference on Network Softwarization (NetSoft)*, 497–502. <https://doi.org/10.1109/NetSoft70012.2026.11603546>
- [14] Kirana, M. C., Keyela, P., Rostamian, F., Tashman, D. H., & Cherkaoui, S. (2026). ML-Enabled Open RAN: A Comprehensive Survey of Architectures, Challenges, and Opportunities (Version 1). arXiv. <https://doi.org/10.48550/ARXIV.2604.01239>
- [15] Lee, S., & Kim, H. (2025). An AI/ML Framework-Driven Approach for Malicious Traffic Detection in Open RAN. *Computer Modeling in Engineering & Sciences*, 145(2), 2657–2682. <https://doi.org/10.32604/cmes.2025.070627>
- [16] Ls, Y. K., Jain, S., Kumar Victor, M. S., Ovais, A., Amalapuram, S. K., Reddy Tamma, B., & Murthy C. S. R. (2026). FALCON++: A Semi-Supervised Anomaly Detection and Localization Framework for Resilient O-RAN Deployments. *2026 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–6. <https://doi.org/10.1109/ICCWorkshops63917.2026.11586571>
- [17] Mahmoud, H. H., Mi, D., Aneiba, A., Idrissi, M., Sharma, G., Foh, C. H., & Xiao, P. (2026). A Review of Open-RAN Intelligence: Opportunities, Challenges, Real-Life Applications and Impacts. *ACM Computing Surveys*, 58(8), 1–36. <https://doi.org/10.1145/3777379>
- [18] Mahrez, Z., Driss, M. B., Sabir, E., Saad, W., & Driouch, E. (2023). Benchmarking of Anomaly Detection Techniques in O-RAN for Handover Optimization. *2023 International Wireless Communications and Mobile Computing (IWCMC)*, 119–125. <https://doi.org/10.1109/IWCMC58020.2023.10183347>
- [19] Moore, J., Abdalla, A. S., Reshi, Z., & Marojevic, V. (2025). Anomaly Detection and Mitigation in O-RAN Networks using an LSTM-RNN Autoencoder and Secure Slicing. *MILCOM 2025 - 2025 IEEE Military Communications Conference (MILCOM)*, 1–6. <https://doi.org/10.1109/MILCOM64451.2025.11310627>
- [20] Nassar, A. W., Aly, H. H., & ElBadawy, H. M. (2026). AI-Driven Intelligent Handover Management in O-RAN: A Multi-xApp Approach for Load Balancing and Anomaly Detection. *2026 43<sup>rd</sup> National Radio Science Conference (NRSC)*, 52–60. <https://doi.org/10.1109/NRSC71102.2026.11556038>
- [21] Navidan, H., Martín, C., Maglogiannis, V., Naudts, D., Díaz, M., Moerman, I., & Shahid, A. (2025). An End-to-End Digital Twin Framework for Dynamic Traffic Analytics in O-RAN. <https://doi.org/10.36227/techrxiv.174494653.36571537/v2>
- [22] Parada, R., Vilajosana, X., Alfayoumi, S., Serra, J., Font-Bach, O., & Dini, P. (2025). An open testbed for O-RAN experimentation with AI-enabled control and monitoring. *Internet of Things*, 33, 101729. <https://doi.org/10.1016/j.iot.2025.101729>
- [23] Rumes, Y., Attanayaka, D., Porabage, P., Pinola, J., Groen, J., & Chowdhury, K. (2024). Federated Learning for Anomaly Detection in Open RAN: Security Architecture Within a Digital Twin. *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 877–882. <https://doi.org/10.1109/EuCNC/6GSummit60053.2024.10597083>
- [24] Santana, M., & Dias, K. L. (2025). Open RAN-Enabled Deep Learning-Assisted Mobility Management for Connected Vehicles. *2025 International Conference on Information Networking (ICOIN)*, 378–383. <https://doi.org/10.1109/ICOIN63865.2025.10992821>
- [25] Shah, S. D. A., Hafeez, M., Salama, A., & Zaidi, S. A. R. (2025). Proactive AI-and-RAN Workload Orchestration in O-RAN Architectures for 6G Networks (Version 1). arXiv. <https://doi.org/10.48550/ARXIV.2507.09124>

### B.Sc. Satya Sumanth Vanapalli

e-mail: sumanthvanapalli074@gmail.com

Satya Sumanth Vanapalli, a computer science student at Siddhartha Academy of Higher Education, has published several journal and conference papers indexed in Scopus on machine learning, computer vision, and precision farming. He holds a patent, leads a startup funded by Acharya N. G. Ranga Agricultural University, and is a Chanakya Fellow from the Indian Institute of Technology Tirupati, focusing on Artificial Intelligence-based agricultural solutions.



### Ph.D. Rajesh Polepogu

e-mail: rajeshpolepogu@vrsiddhartha.ac.in

Rajesh Polepogu is an assistant professor in electronics and instrumentation engineering at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada. He is pursuing a Doctor of Philosophy from Vellore Institute of Technology and holds a master of technology from Jawaharlal Nehru Technological University, Kakinada. His research focuses on bio-signal and statistical processing, he is a reviewer for reputed journals and a life member of several professional societies.



**Ph.D. Parish Venkata Kumar K**

e-mail: kpvk@vrsiddhartha.ac.in

Parish Venkata Kumar K is an assistant professor in the Department of Computer Applications at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada. He specializes in data mining and big data analytics using R. He is a verified academic under Siddhartha Academy of Higher Education (Deemed to be University).

<https://orcid.org/0000-0002-0454-4908>
**Ph.D. Vijayasankar Anumala**

e-mail: vijayasankar.anumala@gmail.com

Vijayasankar Anumala is an associate professor in the Department of Electronics and Communication Engineering at V R Siddhartha School of Engineering, Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. His major research interests include biomedical signal processing and wireless communications.

<https://orcid.org/0000-0002-1483-1708>
**Ph.D. Vinodh Babu Panguluri**

e-mail: panguluri.v@gmail.com

Vinodh Babu Panguluri is an associate professor in the Department of Electronics and Communication at Bapatla Engineering College. His expertise lies in signal and image processing. He has published several papers in reputed conferences and journals.

<https://orcid.org/0000-0003-2911-1479>
**Ph.D. Lakshmi Narayana Jammula**

e-mail: Jln\_9976@yahoo.com

Lakshmi Narayana Jammula is a senior academician with over 25 years of experience in teaching, research, and academic administration in electronics and communication engineering. He currently serves as principal & professor of ECE at Sri Chaitanya Institute of Technology & Research, Ponnkal, and specializes in RF & Microwaves, antennas, DSP, and communication systems, with extensive contributions to research, patents, and accreditation processes.

<https://orcid.org/0009-0006-6551-4434>
**M.Sc. Brahmaiah Madamanchi**

e-mail: madamanchib@gmail.com

Brahmaiah Madamanchi is an assistant professor in the Department of Computer Science & Engineering at RVR & JC College of Engineering, Guntur, Andhra Pradesh, India. His areas of expertise include computer networks, machine learning, and privacy & security in AI.

<https://orcid.org/0000-0001-9938-9914>
**B.Sc. Sravani Duvvu**

e-mail: sravani.duvvu35@gmail.com

Sravani Duvvu is a fourth-year engineering student specializing in electronics and instrumentation engineering at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. Her interests lie in the fields of Internet of Things, machine learning and web programming.

<https://orcid.org/0009-0008-8373-446X>
**B.Sc. Bhanusree Nanduri**

e-mail: bhanusree.nanduri2005@gmail.com

Bhanusree Nanduri is a fourth-year engineering student specializing in electronics and instrumentation engineering at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. Her interests lie in the fields of Internet of Things, machine learning and web programming.

<https://orcid.org/0009-0009-3976-4159>
**B.Sc. Syam Sundar Musinala**

e-mail: musinalasyamsundar2004@gmail.com

Syam Sundar Musinala is a fourth-year engineering student specializing in electronics and instrumentation engineering at Siddhartha Academy of Higher Education (Deemed to be University), Vijayawada, India. His interests lie in the fields of Internet of Things, machine learning and web programming.

<https://orcid.org/0009-0009-9703-3813>
