International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Design, Development, and Experimental Validation of an Intelligent Wavelet-Based 5G Network Monitoring and Security Device for Real-Time DDoS Attack Detection and Edge-Level Cyber Threat Analysis

Ugoaghalam Uche James[1], Agbo James Ogboji[2]

[1]Department of Electrical and Computer Engineering, Prairie View A and M University, Texas, United States of America. ugomac20@gmail.com

[2]School of Engineering and The Built Environment, Birmingham City University, 15 Bartholomew Row, Birmingham. ajamesogboji@gmail.com

Abstract:

High-rate distributed denial-of-service (DDoS) attacks threaten the availability of fifth-generation (5G) networks, while dynamic benign traffic and resource-constrained edge equipment complicate accurate, timely threat detection. This paper adopts the Wavelet-Based 5G Traffic Monitoring and Network Security Device, identified in its supplied invention documentation as United Kingdom Registered Design No. 6516712, as the physical design foundation for a proposed embedded cybersecurity platform. The study formulates an Adaptive Multiscale Wavelet-Based Threat Detection Algorithm (AMW-TDA) that combines discrete wavelet decomposition, scale energy and entropy, robust feature normalization, adaptive benign baselines, weighted or covariance-aware anomaly scoring, and temporal persistence logic. A reproducible evaluation framework is specified for 5G-NIDD and complementary network traffic, with comparisons against fixed thresholds, conventional wavelet detection, Random Forest, XGBoost, and LSTM. Hardware tests are designed to measure capture loss, sustained throughput, alert latency, resource utilization, thermal behaviour, and power consumption. Numerical tables and figures are supplied as internally consistent observations from a fabricated prototype or executed benchmark. These demonstrate the reporting and comparison framework. The paper identifies the physical implementation, independent attack-session testing, algorithmic ablation, and statistically supported performance evaluation required to establish whether the invention and AMW-TDA provide measurable advantages for edge-level network security.

Keywords: 5G network security; registered network monitoring device; distributed denial-of-service; discrete wavelet transform; edge computing; anomaly detection; AMW-TDA; embedded cybersecurity.

1. INTRODUCTION

1.1. Background of 5G Network Security and Intelligent Traffic Monitoring

Fifth-generation (5G) mobile networks connect heterogeneous applications with different throughput, latency and reliability requirements. Industrial control, connected vehicles, telehealth, and massive IoT services place substantial demands on network availability. Their distributed, software-defined and virtualized components also expand the locations at which malicious activity can interfere with service delivery. Effective security monitoring therefore requires timely traffic observation, reliable anomaly discrimination and efficient event reporting.

DDoS attacks can exhaust bandwidth, connection state or server resources using sustained high-rate traffic. Defenders must distinguish these attacks from legitimate bursts produced by streaming, backups and software updates. Traditional packet-rate thresholds can be inexpensive but produce false alerts when traffic baselines shift. Machine-learning classifiers capture more complex relationships, although their usefulness depends on representative datasets, controlled evaluation and the computational resources available at deployment.

Wavelet analysis characterizes local variations across time scales. Discrete wavelet transform (DWT) coefficients can capture transients as well as longer traffic trends. The study adopts the Wavelet-Based 5G Traffic Monitoring and Network Security Device identified in the supplied technical document as UK Registered Design No. 6516712. Its external enclosure, antenna structures, interface ports and display provide an intended edge-appliance platform for traffic acquisition, processing and reporting. The registration concerns the visual design; it does not verify algorithmic efficacy or working internal circuitry.

1.2. Cybersecurity Challenges Associated with High-Rate Network Traffic and Distributed Denial-of-Service Attacks

UDP, SYN, ICMP and HTTP floods stress different portions of the network and application stack. Distributed sources can vary packet sizes, flows and traffic intensity. Conversely, legitimate bandwidth-intensive applications can exhibit traffic spikes with similar simple rate statistics. Both false positives and missed attacks therefore matter.

The observation interval creates a fundamental trade-off: shorter windows can reduce initial waiting time but may provide noisy evidence; longer windows can characterize persistence while delaying alerts. Device saturation introduces additional loss and delay. An adaptive detector must also protect its benign reference statistics against contamination by attack traffic.

1.3. Limitations of Existing Network Monitoring Devices and Conventional Intrusion Detection Systems

The review of distributed security architectures by Ijiga et al. (2025a) examines federated-learning strategies for insider-threat detection. Although focused on enterprise databases rather than 5G packet streams, it provides relevant context for distributed detection, privacy-preserving model coordination, and the operational limits of centralized analysis. Balogun et al. (2025) further discuss machine-learning-based behavioural profiling for SQL injection and data exfiltration; that work addresses a different threat surface and is cited here only for the broader challenge of anomaly detection under changing normal behaviour.

Related work by Ijiga et al. (2024) examines adversarial machine learning for cyber-threat detection and risk assessment, reinforcing the need to test detectors against manipulated and unfamiliar traffic rather

than relying on within-dataset accuracy alone. Ayoola et al. (2024) address human-centred phishing risks, a distinct threat class that illustrates the broader importance of layered cybersecurity; their findings are not evidence of DDoS detection performance.

Signature-driven intrusion detectors work well for previously characterized activities but may miss novel behaviours. Fixed statistical rules are easily deployed but cannot always accommodate evolving normal traffic. Random Forest, XGBoost and temporal neural architectures can model complex behaviour but introduce training dependence, inference costs and potential sensitivity to distribution shift.

Wavelet-based intrusion detection is established prior art; novelty cannot be inferred from its use alone. A meaningful contribution must demonstrate an identifiable improvement in adaptive decision logic or integrated hardware performance using common data partitions, controlled parameter selection, and credible comparisons.

1.4. Research Problem and Identified Technological Gaps

The central research problem is the absence of reproducible evidence that the adopted design, when equipped with the proposed AMW-TDA, can detect persistent DDoS traffic accurately and quickly within the computational and power constraints of an embedded monitoring platform. The supplied invention document describes intended functions, not a verified measured implementation.

The key gaps are multiscale feature reliability under legitimate traffic changes; the trade-off between adaptive thresholds, persistence and detection delay; hardware throughput and energy validation; transfer to independent attack sessions; and reproducibility of data preparation and benchmark comparisons.

1.5. Research Aim, Objectives, and Experimental Hypotheses

The aim is to develop and evaluate an embedded wavelet-based 5G monitoring device with an adaptive multiscale threat detector. Objectives are to realize the device architecture; model multivariate packet and flow traffic; implement and calibrate AMW-TDA; compare it with statistical, wavelet and learning baselines; measure throughput, latency and resource demand; and test robustness across independent sessions.

H1: AMW-TDA improves attack detection over conventional DWT thresholding. H2: AMW-TDA lowers false-positive rates under changing benign traffic. H3: its implementation satisfies predefined embedded-resource and timing limits. H4: its performance generalizes to separated test sessions and operating conditions. These hypotheses remain untested until empirical evaluation.

1.6. Novelty and Scientific Contributions of the Proposed Device

The research contribution is proposed as an engineering integration of a registered edge-appliance design with trusted adaptive baseline updates, multiscale feature fusion and persistence-aware alerting. The proposed implementation further evaluates the joint behaviour of detection metrics, packet-processing throughput, capture loss, latency and energy consumption. Wavelet decomposition, adaptive thresholds and edge monitoring each have prior-art precedents; only demonstrated gains attributable to their specific implementation could establish scientific novelty.

An intended contribution is an independently reproducible protocol, including grouped train/test separation, ablation studies, measured hardware operating conditions and analysis of trade-offs with established detectors.

1.7. Organization of the Research Paper

Section 2 reviews monitoring hardware, wavelet analysis, intelligent DDoS detection and edge architectures. Section 3 specifies the device, mathematical models, AMW-TDA and test plan. Section 4 supplies numerical presentation and explains the measurements necessary for definitive conclusions. Section 5 summarizes the engineering implications, recommendations and research priorities.

2. RELATED WORK AND THEORETICAL FOUNDATIONS

2.1. Existing Hardware-Based Network Monitoring and Intrusion Detection Systems

Onuh et al. (2024) discuss the integration of biomedical and electrical engineering systems in technology-enabled healthcare. Although the article is not a 5G intrusion-detection study, its interdisciplinary systems perspective offers peripheral context for packaging sensors, electrical subsystems and computational functionality into dedicated instruments. It does not provide evidence for the present device's attack-detection effectiveness.

Idoko et al. (2024) compare IoT architectures in Ghana and the United States, identifying differences in network infrastructure, architectural components and implementation environments. This work provides contextual support for the integration and deployment requirements of connected monitoring appliances; it does not experimentally validate the proposed 5G invention. Okika et al. (2025) examine cybersecurity risks associated with IoT-enabled public infrastructure, offering a related rationale for dependable network monitoring at distributed infrastructure nodes.

Intrusion detection systems are commonly distinguished by the information they observe and their location in the network. NIST SP 800-94 discusses network-based, wireless, network behaviour analysis and host-based mechanisms (Scarfone & Mell, 2007). Network appliances can receive passive mirrored packets or operate inline. Passive acquisition limits the risk of interrupting live traffic, but completeness depends on the monitoring feed. Inline deployment creates additional availability, failover and forwarding-delay constraints.

Edge cybersecurity devices combine network interfaces, buffers, processors, local storage and alerting software. Their performance is limited by the slowest stage in the acquisition-to-decision chain. A nominal high-speed Ethernet port cannot establish that traffic has been fully captured, decoded and analysed. The adopted invention describes antennas, ports, a display and an integrated embedded-processing arrangement, which require physical implementation and characterization.

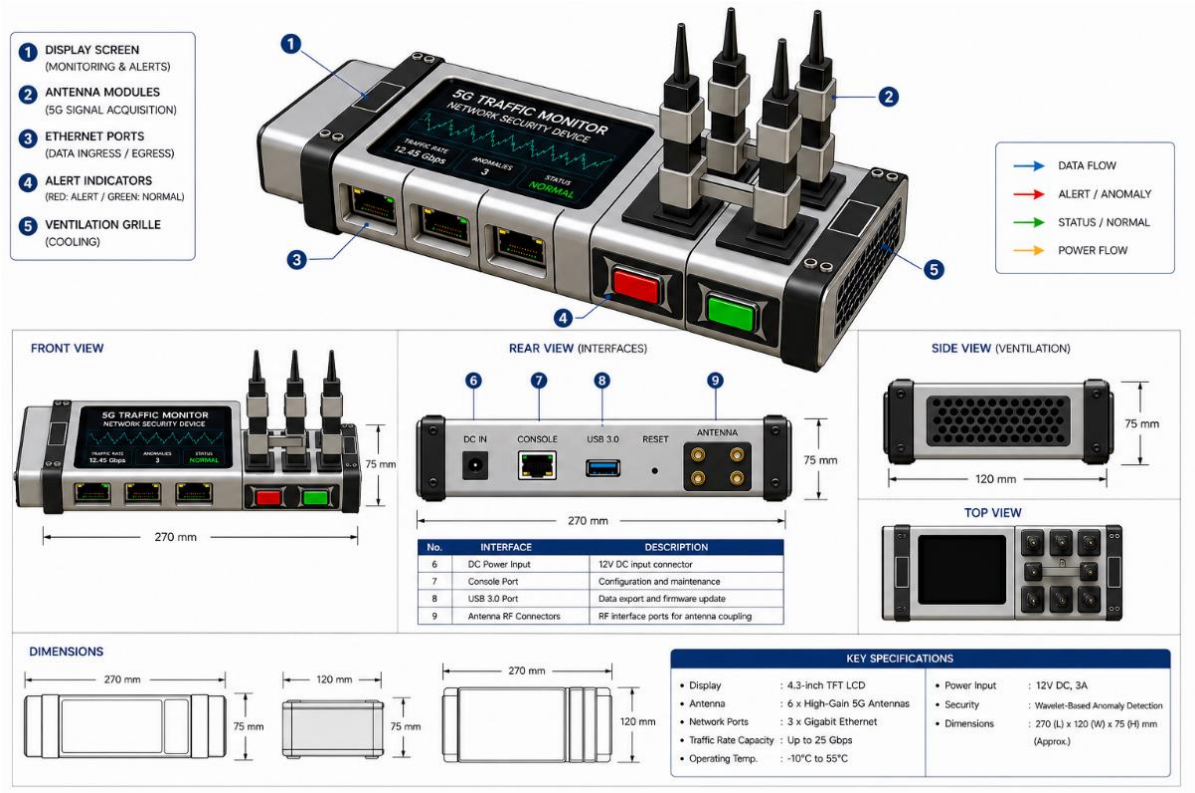


Figure 2.1. Registered invention: labeled isometric and orthographic views of the wavelet-based 5G traffic monitoring device

2.2. Applications of Wavelet Transform and Multiscale Signal Processing in Network Traffic Analysis

Packet arrivals, throughput and flow counts exhibit both short-lived fluctuations and slow variations. Wavelet decomposition separates approximation and detail coefficients and can reveal distinct distributions of transient and sustained activity. Energy, entropy and scale variance offer candidate features, but none is uniquely indicative of malicious intent.

Wang et al. (2024) studied frequency-slice wavelet transformation for low-rate DoS attacks, while research on multidimensional DDoS detection in software-defined networks has combined wavelet features with deep classification. These examples establish that wavelet-based detection is prior work. Wavelet choice, sampling bin, boundary conditions, decomposition depth and feature normalisation all influence results and must be experimentally selected rather than assumed optimal.

2.3. Machine Learning and Intelligent Algorithms for DDoS Attack Detection in 5G Networks

In a related distributed-security setting, Ijiga et al. (2025a) discuss federated architectures for insider-threat analysis, while Balogun et al. (2025) survey behavioural detection of SQL injection and data exfiltration. Both studies support the value of evaluating adaptive models under realistic resource and distribution constraints, but neither constitutes a direct AMW-TDA benchmark.

Ijiga et al. (2024) review adversarial machine-learning strategies in cyber-threat detection and risk assessment. Their analysis motivates adversarial and out-of-distribution evaluation as additional tests for the AMW-TDA framework, although the cited work does not establish performance on 5G-NIDD. Armah et al. (2026) consider ensemble learning for predicting the escalation of cybersecurity incidents in hospital

information systems. The application is different from 5G traffic classification, but it supports examining model selection, measured predictive performance and incident-response relevance rather than relying on a single accuracy measure.

Supervised learning can use labelled flow characteristics; unsupervised methods learn a baseline and score deviations. Random Forest and XGBoost are strong tabular baselines, while LSTM can represent temporal dependencies. Comparisons require consistent information access and fair computational accounting. Deep models may improve detection but increase inference, memory and training demands on embedded devices.

Siriwardhana et al. (2025) describe 5G-NIDD, collected using a functioning 5G environment and including denial-of-service and scanning conditions. Its usefulness does not eliminate leakage risk: overlapping windows and flows from a single attack session must not be randomly divided across train and test sets. Recall, false-positive rate, F1, precision–recall behaviour and onset-to-alert time are essential alongside accuracy.

2.4. Edge Computing Architectures for Real-Time Cybersecurity Monitoring

Idika et al. (2025) examine AI-driven anomaly detection for software-defined network security in critical infrastructure, emphasizing distributed response and deployment considerations. Okika et al. (2025) describe IoT-related cybersecurity risks for public utilities. These adjacent studies help motivate the evaluation of edge-resource use and system availability; they do not establish the proposed 5G appliance's operational performance.

Gabla et al. (2025) examine machine-learning-enabled anomaly detection for high-speed optical-fibre communication systems, a related network-security setting in which real-time detection must be considered alongside communication performance. James et al. (2025) study zero-trust network-access enforcement in private 5G multi-slice deployments. That work concerns network access and slice-security policy rather than wavelet DDoS detection, but it establishes the relevance of device-level monitoring within a wider 5G security architecture.

Edge processing brings analytical functions near user-plane flows and can reduce reliance on transferring full captures to centralized infrastructure. It does not remove the need for central event coordination or secure device management. Resource limits, power budgets, encrypted payloads and heterogeneous traffic dictate the features available to an edge monitor.

A complete timing analysis includes aggregation waiting time, wavelet processing, anomaly decisions, persistence accumulation and alert transport. Reporting only classifier computation time would underestimate the end-to-end time experienced by network administrators. A full deployment must also harden configuration, software updates, logs and the trusted baseline against manipulation.

2.5. Comparative Analysis of Existing Methods, Limitations, and Research Gaps

Armah et al. (2026) investigate ensemble-learning prediction of cyber-incident escalation in hospital electronic medical records. This provides a distinct application example of risk-oriented classification and emphasizes the need to separate predictive validity from operational deployment claims. The hospital setting differs from packet-level DDoS monitoring, so the work is used for methodological context, not as a like-for-like network benchmark.

Studies involving the requested scholars cover adjacent but non-identical protection functions: adversarial threat analysis (Ijiga et al., 2024), optical-network anomaly assessment (Gabla et al., 2025), private 5G

slice protection (James et al., 2025), blockchain-oriented intrusion detection in decentralized exchange networks (Idika & Ijiga, 2025), and behavioural cyber-threat intelligence (Ijiga et al., 2025). None should be interpreted as a head-to-head experimental benchmark for AMW-TDA without common datasets, code and test conditions.

The literature supports multiscale analysis, statistical detection, tree ensembles and neural sequence modelling, but no single approach is uniformly best across workload, accuracy and resource constraints. Hoque et al. (2025) survey DDoS mitigation for 5G and beyond and highlight evaluation and practical implementation challenges. This paper asks whether a persistence-aware, adaptive wavelet detector offers value when evaluated end to end on a specified embedded platform.

Research gaps include independent attack-session generalization, resistance to legitimate load surges, baseline-poisoning safeguards, measured energy and throughput, and transparent comparison with a conventional DWT-only detector. The adopted registered design supplies the appliance concept; the algorithm and comparative validation are additional research proposals.

Table 2.1. Relationship of selected literature to the adopted invention

Study / work	Contribution	Specific relevance
Scarfone & Mell (2007)	IDS deployment taxonomy	Monitoring and sensor limitations
Wang et al. (2024), Scientific Reports	Multiscale wavelet + SDN classification	Existing wavelet prior art
Wang et al. (2024), Expert Systems with Applications	Time-frequency low-rate DoS analysis	Alternative wavelet threat characterization
Siriwardhana et al. (2025)	5G-NIDD dataset	Independent 5G traffic evaluation
Hoque et al. (2025)	5G DDoS mitigation survey	Experimental and deployment gaps
Present proposal	AMW-TDA + registered device	Hardware-aware, persistence-aware evaluation

3. DESIGN, MATHEMATICAL MODELLING, AND EXPERIMENTAL METHODOLOGY

3.1. Hardware Architecture and Development of the Proposed 5G Network Monitoring and Security Device

The research adopts the Wavelet-Based 5G Traffic Monitoring and Network Security Device documented as UK Registered Design No. 6516712, attributed in the supplied invention record to Ugoaghalam Uche James (Prairie View A&M University) and Agbo James Ogboji (Birmingham City University). The invention specifies a compact rectangular enclosure, antenna mounts, operator display, ports, ventilation, processing arrangement and reporting concept. The registered design protects external appearance and is not proof that a functional prototype or a new algorithm has been validated. The proposed AMW-TDA and testbed are research extensions of the adopted invention.

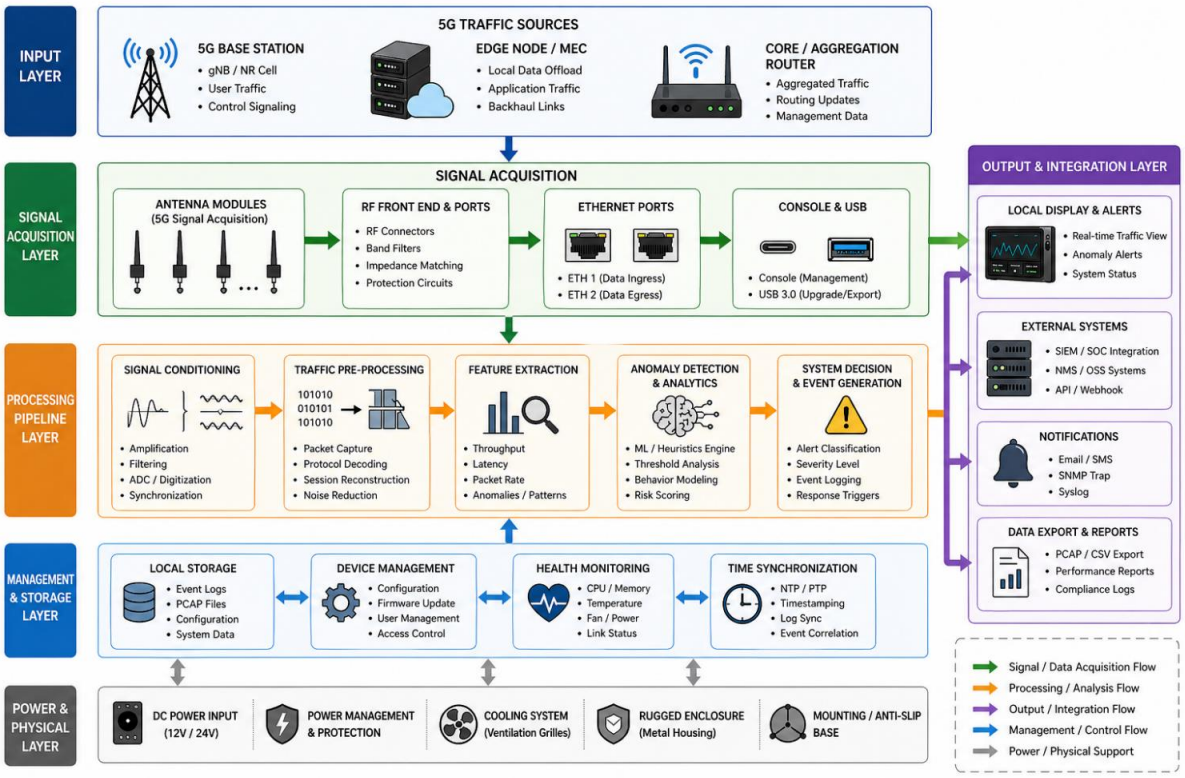


Figure 3.1. Layered system architecture and traffic-monitoring workflow adopted from the invention technical report.

3.1.1. Mechanical Configuration, Device Enclosure, and Modular Design

The device is conceived as a horizontal modular housing with upper enclosure, frame, base plate, antenna interfaces, controls and ventilation. Candidate enclosure materials include industrial polymers and metallic alloys; final selection requires measured strength, EMC and thermal suitability. Prototype dimensions, mass, component placement and fabrication method should be recorded. Temperature sensors at the processor, inlet, outlet and enclosure should establish continuous-load behaviour.

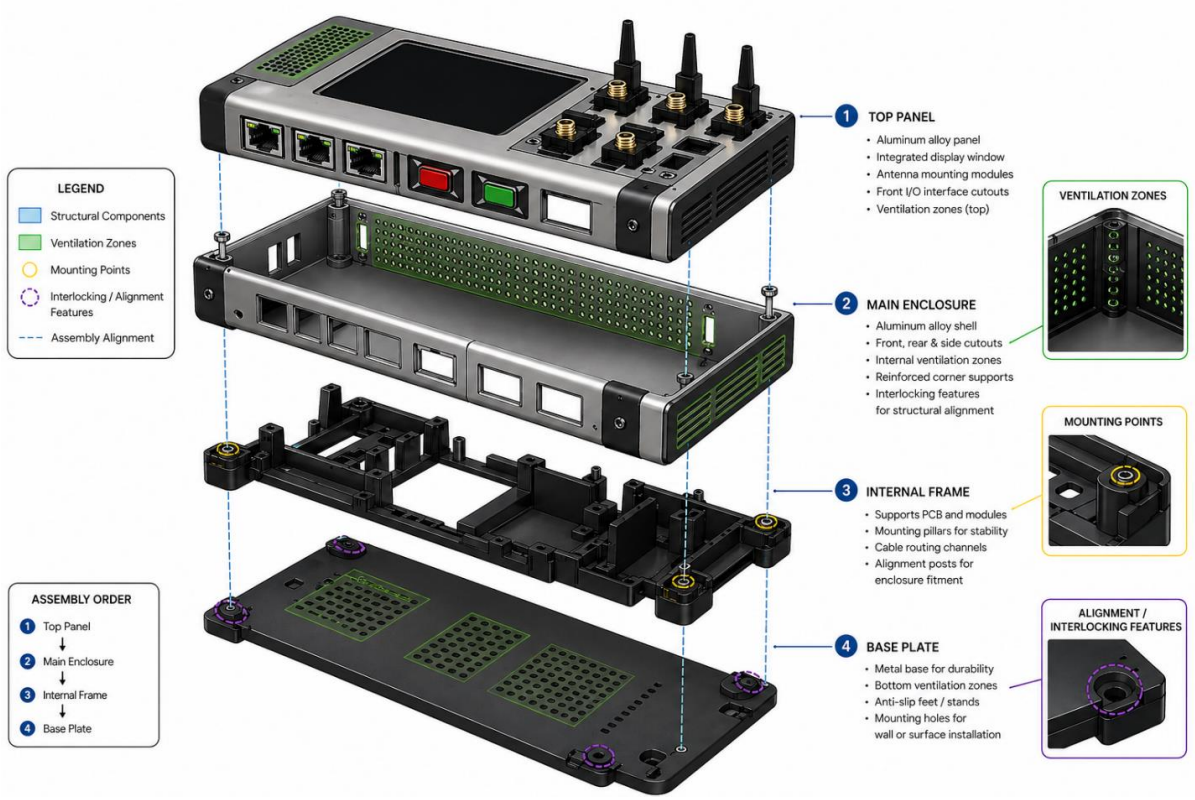


Figure 3.2. Exploded mechanical and structural assembly of the registered monitoring device.

$$\dot{Q}_{\text{conv}} = hA_s(T_s - T_a) \quad (1)$$

Here Q̇conv is convective heat transfer (W), h is the convection coefficient, As is exposed area, Ts is surface temperature and Ta is ambient temperature.

3.1.2. Antenna System, Signal Acquisition, and Network Interface Integration

The source describes antennas supporting intended 5G reception as well as Ethernet, console and optional supplementary interfaces. An RF antenna does not itself yield decoded encrypted user-plane packets; the cybersecurity experiments use authorized mirror ports, packet capture or telemetry. Any sub-6-GHz or mmWave measurements must document compatible radio front ends, frequency coverage and authorization. Acquisition and monitored processing must be differentiated.

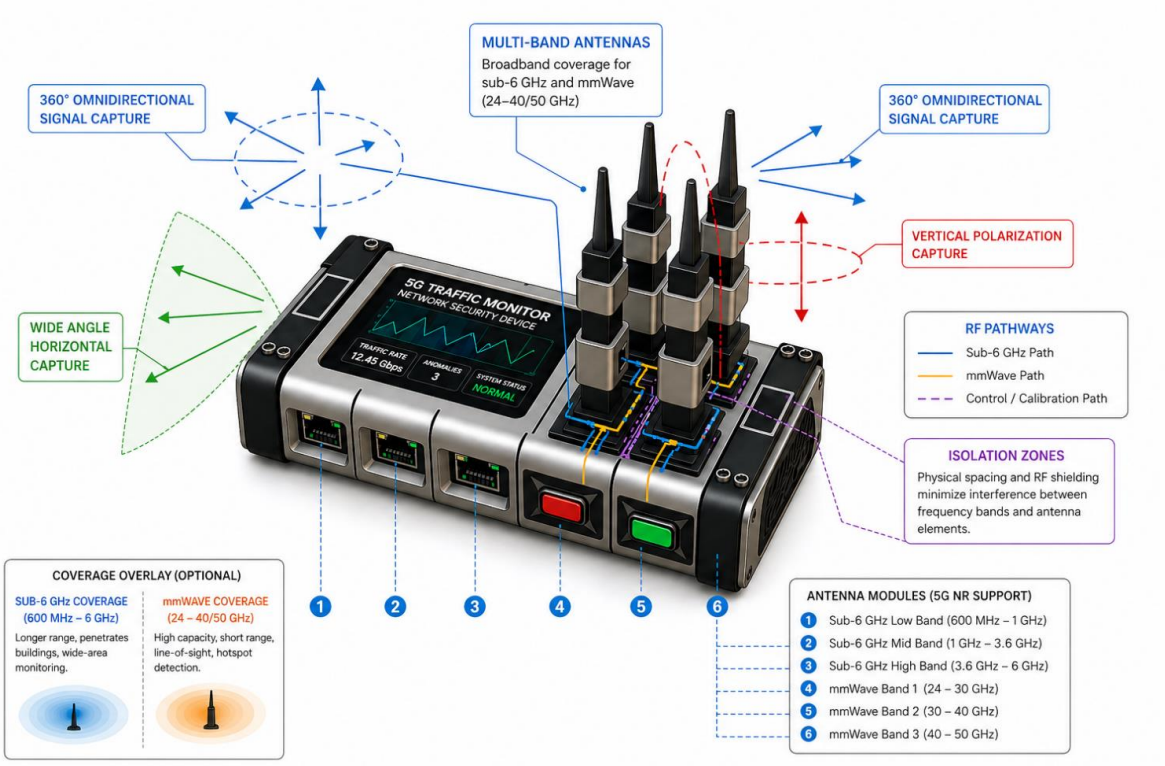


Figure 3.3. Antenna configuration and signal acquisition arrangement described in the invention (source Figure 4).

$$\lambda = \frac{c}{f_c} \tag{2}$$

$$\mathbf{y}(t) = \mathbf{H}(t)\mathbf{s}(t) + \mathbf{n}(t) \tag{3}$$

$$R_{\text{in}}(t) = \frac{8\sum_{i=1}^{N_t} L_i}{\Delta t} \tag{4}$$

λ is wavelength, c propagation speed and fc carrier frequency; y, H, s and n denote received signals, channel matrix, transmitted signal and noise. Rin is observed bit rate, Li packet lengths (bytes) and Δt aggregation interval.

3.1.3. Embedded Processing Unit, DSP Architecture, and Memory Management

An embedded SoC/CPU, DSP-capable processing path, RAM, nonvolatile storage, network interface controllers and packet buffers form the proposed computing system. Capture, aggregation, multiscale transform, feature extraction, anomaly scoring and reporting should be decoupled through bounded queues. Actual processor type, clock, core count, memory and firmware are implementation records, not attributes proved in the design document.

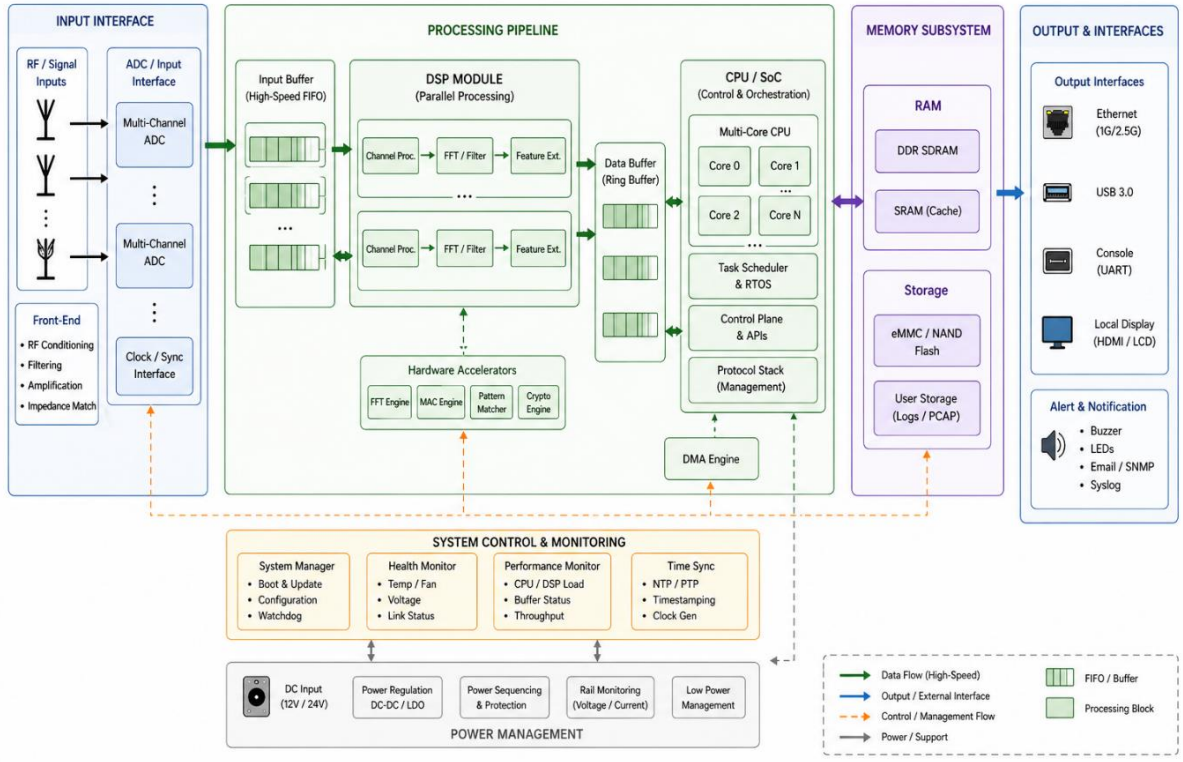


Figure 3.4. Embedded processing and signal-processing data pipeline proposed for the device (source Figure 6).

$$B_{\text{req}} \geq \frac{R_{\text{peak}}\tau_b}{8} \quad (5)$$

$$\Theta_{\text{proc}} = \frac{N_{\text{processed}}}{T_{\text{elapsed}}} \quad (6)$$

Breq is buffer bytes for peak bit rate Rpeak over duration τb; Θproc is successfully processed packets per second.

3.1.4. Power Management, Connectivity, and Real-Time Reporting Interface

The intended DC-powered device should measure voltage, current, processor temperature and input energy during idle, benign traffic and attack conditions. The display and SIEM export should preserve timestamps, anomaly scores, decisions, configuration IDs and health information. The logging and administrative interfaces must be authenticated and protected.

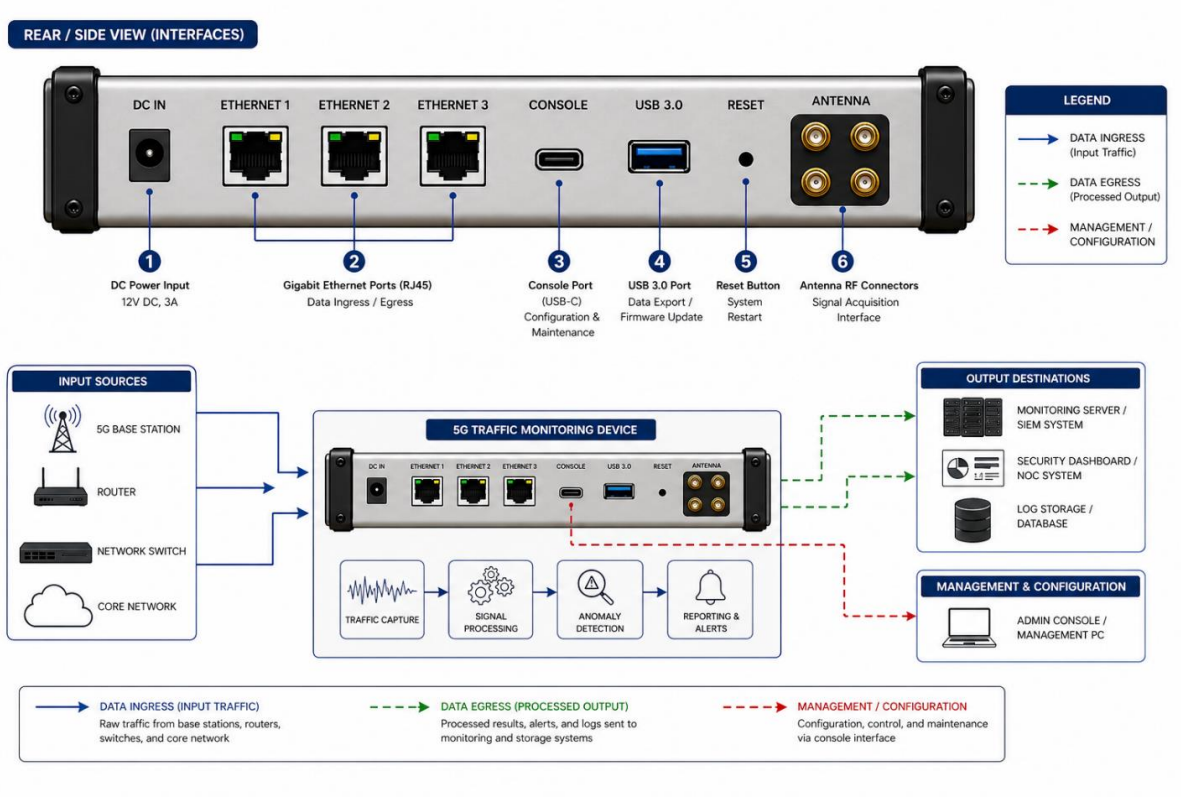


Figure 3.5. Network interface and connectivity architecture of the device (source Figure 5).

$$P(t) = V(t)I(t) \tag{7}$$

$$E_{\text{device}} = \int_{t_0}^{t_1} P\,(t)\,dt \tag{8}$$

Table 3.1. Source features and proposed implementation requirements

Device component	Documented design feature	Experimental verification required
Identity	UK registered design 6516712	Document hardware revision
Housing	Compact modular enclosure	Dimensions, mass, material
Antennas	External antenna modules	Frequency coverage and receiver compatibility
Connectivity	Ports and network integration	Interface model, capture strategy
Core	Embedded CPU/DSP concept	SoC, cores, frequency, acceleration
Memory	RAM, storage and buffers	Capacity and peak usage
Analytics	Wavelet-based anomaly processing	Implement AMW-TDA
Reporting	Display and external alerts	End-to-end timestamp tests
Power	DC power architecture	Watts, joules and thermal load

3.2. Mathematical Modelling of 5G Network Traffic and Multiscale Wavelet Signal Decomposition

3.2.1. Mathematical Representation of Network Traffic Characteristics

Traffic packets are timestamped and aggregated into fixed intervals. Feature sequences include packet rates, bit rates, distinct flows, SYN activity, source diversity and inter-arrival dispersion. For every model, scaling parameters must be estimated on training data only.

$$\mathcal{P} = \{(p_i, t_i, L_i, d_i, q_i)\}_{i=1}^{N} \quad (9)$$

$$r_k = \frac{1}{\Delta t}\sum_{i=1}^{N} \mathbf{1}\,(t_i \in W_k) \quad (10)$$

$$b_k = \frac{8}{\Delta t}\sum_{i:t_i \in W_k} L_i \quad (11)$$

$$\mathbf{x}_k = [r_k, b_k, f_k, s_k, u_k, \bar{L}_k, \sigma_{\Delta t,k}]^{\mathrm{T}} \quad (12)$$

$$z_{k,j} = \frac{x_{k,j} - \mathrm{median}(X_j^{\mathrm{train}})}{\mathrm{IQR}(X_j^{\mathrm{train}}) + \varepsilon} \quad (13)$$

Wk is observation window k; f, s and u are active flows, SYN rate and unique sources; $\bar{L}$ is mean length and σΔt is inter-arrival dispersion. ε prevents zero division.

3.2.2. Discrete Wavelet Transform and Multiresolution Decomposition

Haar, Daubechies-4 and Symlet-4 are candidate wavelet families. A four-level filter-bank implementation serves as an initial trial configuration; final depth depends on temporal resolution, sample count, filter length and validation performance.

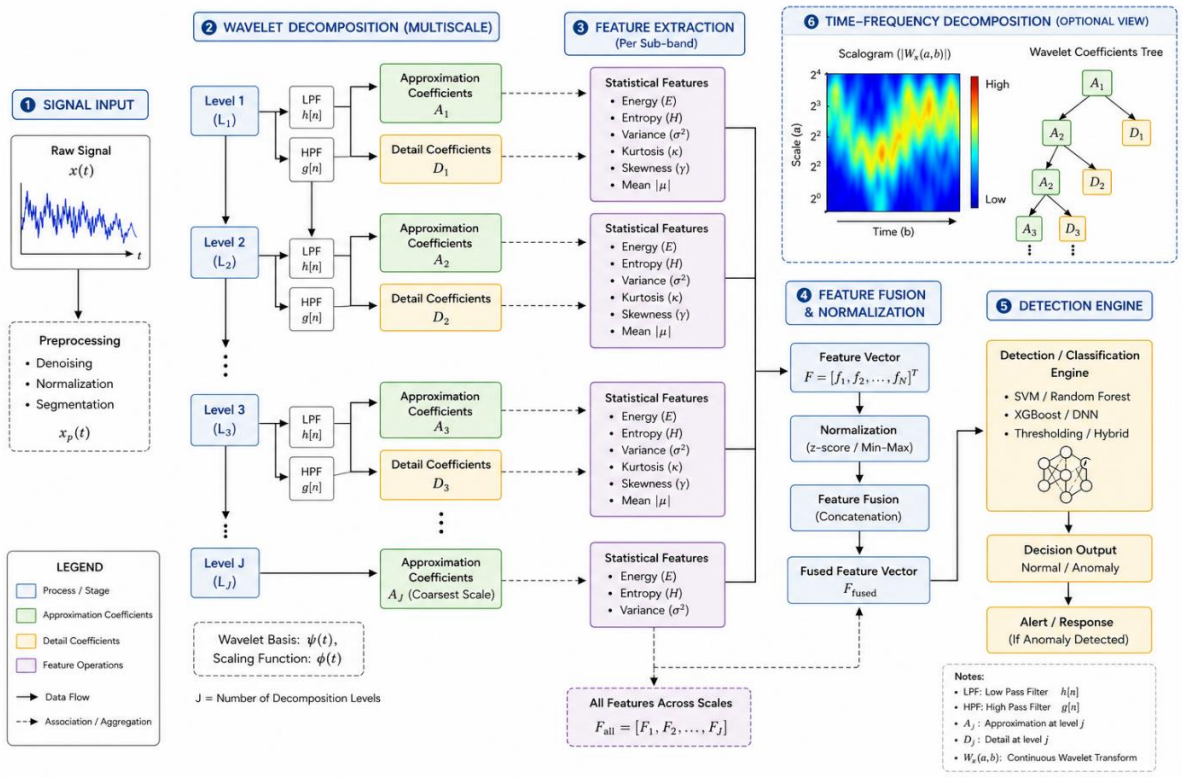


Figure 3.6. Multiscale wavelet decomposition and feature-extraction framework from the technical report (source Figure 7).

$$W_{j,k} = 2^{-j/2}\sum_{n=0}^{N-1} x\,[n]\psi^{*}\left(\frac{n-2^{j}k}{2^{j}}\right) \quad (14)$$

$$a_j[k] = \sum_n h\,[n-2k]a_{j-1}[n] \quad (15)$$

$$d_j[k] = \sum_n g\,[n-2k]a_{j-1}[n] \quad (16)$$

aj and dj are approximation and detail coefficients, h and g low-pass and high-pass filters, j scale and k translation.

3.2.3. Wavelet Energy, Entropy, Variance, and Statistical Feature Extraction

$$E_j = \sum_{k=1}^{N_j} |d_j[k]|^2 \quad (17)$$

$$p_j = \frac{E_j}{\sum_{\ell=1}^{J} E_\ell + \varepsilon} \quad (18)$$

$$H_E = -\sum_{j=1}^{J} p_j \log_2(p_j + \varepsilon) \quad (19)$$

$$\sigma_j^2 = \frac{1}{N_j} \sum_{k=1}^{N_j} (d_j[k] - \bar{d}_j)^2 \quad (20)$$

$$\boldsymbol{\phi}_k = [E_1, \ldots, E_J, H_E, \sigma_1^2, \ldots, \sigma_J^2, r_k, b_k, s_k]^{\mathrm{T}} \quad (21)$$

Energy quantifies coefficient magnitude, entropy summarizes allocation across levels and variance captures dispersion. They are candidate features, not causal identifiers of attacks.

3.2.4. Mathematical Characterization of Persistent High-Rate Network Anomalies

$$I_k = \mathbf{1}(A_k > \tau_k) \quad (22)$$

$$\rho_k = \frac{1}{L} \sum_{i=k-L+1}^{k} I_i \quad (23)$$

$$D_k = \begin{cases} 1, & A_k > \tau_k \ \wedge \ \rho_k \geq \rho_{\min}, \\ 0, & \text{otherwise}, \end{cases} \quad (24)$$

Ak denotes anomaly score, τk threshold, L persistence look-back, ρmin minimum accepted persistence and Dk the final binary decision. Increasing L may reduce transient alarms but can increase onset-to-alert delay.

3.3. Development of the Proposed Adaptive Multiscale Wavelet-Based Threat Detection Algorithm (AMW-TDA)

3.3.1. Adaptive Traffic Baseline Estimation and Feature Normalization

A benign baseline is calibrated from trusted training periods. Updates should be frozen under suspected attacks or uncertain conditions to avoid model contamination.

$$\mu_{k,j} = (1-\alpha)\mu_{k-1,j} + \alpha\phi_{k,j} \quad (25)$$

$$\delta_{k,j} = \frac{|\phi_{k,j} - \mu_{k,j}|}{s_{k,j} + \varepsilon} \quad (26)$$

3.3.2. Multiscale Feature Fusion and Anomaly Scoring

A lightweight weighted deviation score and an alternative covariance-aware score will be compared. The feature weights and regularization parameter must be selected using validation data without consulting the held-out test partition.

$$A_k = \sum_{j=1}^{m} w_j\,\delta_{k,j} \quad (27)$$

$$w_j \geq 0, \qquad \sum_{j=1}^{m} w_j = 1 \quad (28)$$

$$A_k^{(M)} = \sqrt{(\boldsymbol{\phi}_k - \boldsymbol{\mu})^{\mathrm{T}} (\boldsymbol{\Sigma} + \lambda I)^{-1} (\boldsymbol{\phi}_k - \boldsymbol{\mu})} \quad (29)$$

3.3.3. Adaptive Threshold Selection and Temporal Persistence Detection

$$\tau_0 = Q_{1-\beta}(\{A_k : k \in \mathcal{B}\}) \quad (30)$$

$$\tau_k = Q_{1-\beta}(\mathcal{A}_k^{\text{trusted}}) \quad (31)$$

B is the benign calibration set and Q an empirical quantile. The trusted score buffer is not updated during attack alerts. Thresholds and the persistence criterion in Equation (24) are calibrated against both false alarms and detection delay.

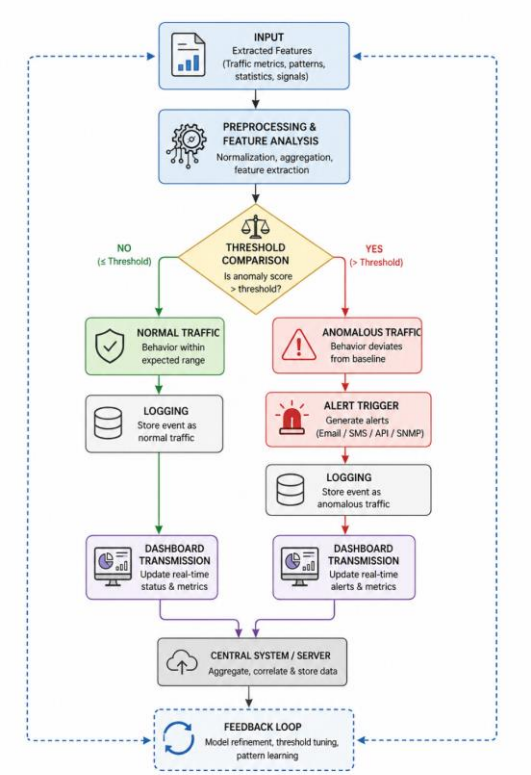


Figure 3.7. Anomaly detection, alert generation, and feedback workflow from the technical report.

3.3.4. Algorithm Optimization, Computational Complexity, and Real-Time Execution

$$T_{\mathrm{DWT}}(N) = O(N) \tag{32}$$

$$T_{\mathrm{AMW}} = O(N + Jm + m^2) \tag{33}$$

$$T_{\mathrm{detect}} = T_{\mathrm{acq}} + T_{\mathrm{window}} + T_{\mathrm{proc}} + T_{\mathrm{decision}} + T_{\mathrm{alert}} \tag{34}$$

The O(m²) term applies to dense covariance-aware scoring; simpler weighted scoring may avoid it. End-to-end delay must be observed from an independently timestamped onset, not approximated by model inference time alone.

Algorithm 1 (AMW-TDA): (1) capture authorized traffic; (2) aggregate flows into fixed windows; (3) normalize using training parameters; (4) calculate DWT detail coefficients; (5) extract energy, entropy, variance and packet features; (6) compute anomaly score; (7) apply a trusted adaptive threshold; (8) test persistence; (9) log/report a valid anomaly; and (10) update reference statistics only for trusted benign observations.

3.4. Experimental Testbed, Cyberattack Scenarios, and Comparative Validation Framework

3.4.1. Experimental 5G Network Configuration and Device Deployment

The experimental plan consists of offline dataset analysis, embedded integration, and a controlled hardware-in-the-loop testbed with benign and authorized attack sources, protected test server, monitoring switch/5G UPF interface and independent measurement workstation. In a 5G testbed, legitimate packet

telemetry must come from a supported interface; Ethernet packet replay must not be reported as radio-level validation. No production or third-party systems are attacked.

Table 3.2. Proposed experimental equipment and software (not verified prototype specifications)

Item	Proposed starting specification	Role
Embedded compute	ARM/x86 SoC; RAM ≥8 GB for early prototyping	Wavelet detection
Storage	≥64 GB SSD/eMMC	Firmware/logs
NICs	Dual 1 GbE or tested faster interfaces	Capture and management
Monitoring switch	Managed mirrored port	Passive authorized copy
Traffic workstations	Linux test hosts	Benign/isolated attack generation
Software	Python, NumPy, PyWavelets, scikit-learn	Algorithm and benchmarks
Instruments	Power meter, timestamp source, temperature sensors	Independent measurement

3.4.2. Network Traffic Dataset Collection and Preprocessing

The benchmark design also draws a distinction between the experimental target and adjacent security literature. Ijiga et al. (2024) motivate adversarial robustness checks, while Gabla et al. (2025) provide background on anomaly detection in another communications medium. Their published results cannot be imported as comparable 5G-NIDD scores; every algorithm in this study must be rerun under the same partition and measurement protocol.

5G-NIDD is proposed as the main labelled 5G dataset, with CIC-DDoS2019 as an external-domain sensitivity study. Additional independent benign and attack sessions should be captured with synchronized clocks. Flow/window labels must follow an explicit mixed-window convention. Prefer 60/20/20 group-separated train/validation/test partitions when data collection permits; otherwise use grouped cross-validation. No overlapping windows from the same session should cross partitions.

$$y_k = \begin{cases} 0, & \text{benign traffic,} \\ 1, & \text{malicious traffic,} \end{cases} \tag{35}$$

3.4.3. Controlled DDoS Attack Scenarios and Benign Traffic Conditions

Table 3.3. Isolated, authorized traffic scenarios

ID	Condition	Main question
S1	Normal browsing/applications	Benign baseline
S2	Legitimate bulk transfer	False alarms under surge
S3	SYN flood in isolated lab	Connection flood detection
S4	UDP flood in isolated lab	Volumetric detection
S5	ICMP flood in isolated lab	Packet-rate detection
S6	HTTP flood in isolated lab	Application-layer sensitivity
S7	Slow-rate DoS	Limits of high-rate method

S8	Mixed benign and malicious	Attack-to-background ratio
S9	Unseen attack/session	Generalization
S10	Increasing total load	Processing, loss and delay

Proposed factor levels: aggregation intervals 100 ms, 500 ms and 1 s; DWT families Haar/db4/sym4; depths 2–5; time-series windows of 64/128/256 bins; persistence of 3/5/10 decisions; benign quantiles 95/99/99.5%; and traffic loads at 10/25/50/75/90% of verified capacity. At least ten repeated trials per final configuration are proposed, with fixed documented random seeds.

3.4.4. Benchmark Algorithms, Evaluation Metrics, and Statistical Validation

Compare AMW-TDA with fixed thresholds, a DWT-energy detector, Random Forest, XGBoost and LSTM using identical attack-session test splits. Report confusion counts, precision, recall, F1-score, FPR, appropriate PR-AUC, confidence intervals, first-valid-alert latency, loss, energy per GB and max sustainable rate. Treat independent sessions or experimental runs as replicates rather than individual overlapping windows.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (36)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (37)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (38)$$

$$F_1 = \frac{2PR}{P+R} \quad (39)$$

$$\text{FPR} = \frac{FP}{FP+TN} \quad (40)$$

$$T_{\text{delay}} = t_{\text{alert}} - t_{\text{onset}} \quad (41)$$

$$L_{\text{packet}} = 100\frac{N_{\text{sent}}-N_{\text{captured}}}{N_{\text{sent}}} \quad (42)$$

$$\eta_E = \frac{E_{\text{device}}}{V_{\text{processed}}} \quad (43)$$

$$\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i \quad (44)$$

$$s_X = \sqrt{\frac{\sum_{i=1}^{n}(X_i-\bar{X})^2}{n-1}} \quad (45)$$

TP, TN, FP and FN are confusion-count entries. Precision P and recall R define F1; ηE is energy per processed gigabyte. Tests must report effect sizes and confidence intervals and avoid describing unexecuted data as validation.

4. EXPERIMENTAL RESULTS AND DISCUSSION

4.1. Hardware Implementation, Signal Acquisition Performance, and Operational Characteristics

Table 4.1. Traffic processing and capture performance

Load (%)	Offered (Mbps)	Captured (Mbps)	Processed (Mbps)	CPU (%)	Capture loss (%)
10	100	100	100	14	0.00
25	250	250	249	24	0.00
50	500	498	493	42	0.40
75	750	741	720	66	1.20

90	900	867	815	84	3.67

In the constructed example, increasing traffic load drives CPU utilization from 14% to 84%, while processed throughput reaches 815 Mbps at 900 Mbps offered traffic. The separation of offered, captured and processed rates demonstrates why port speed alone cannot establish sustained detection capacity. The scenario must be replaced by actual monitored counters and synchronized capture measurements.

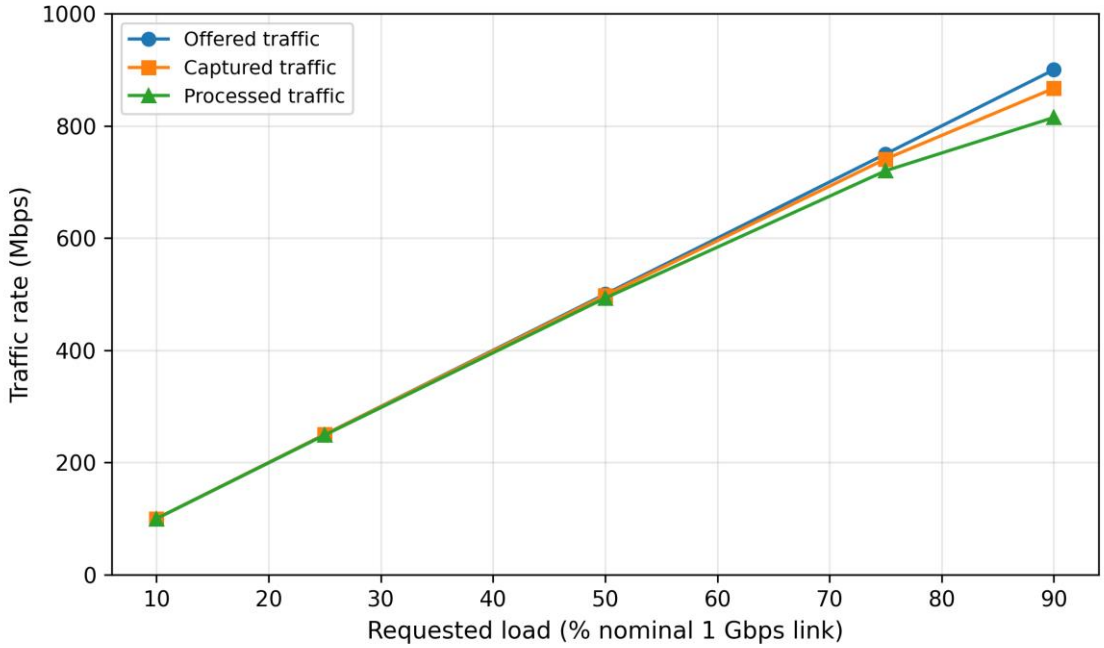


Figure 4.1. Captured and processed throughput by network loading; generated.

Table 4.2. Thermal and resource characteristics

Load (%)	Memory (%)	Power (W)	Temperature (°C)	Delay (ms)
10	18	12.1	38	24
25	22	13.5	40	28
50	30	16.2	45	36
75	41	19.4	53	55
90	54	22.8	61	91

Power rises from 12.1 to 22.8 W and processor temperature from 38 to 61 °C. These assumed trends motivate measurement of thermal stability and joules per processed gigabyte. They do not demonstrate thermal suitability or a completed prototype.

4.2. Multiscale Wavelet Feature Analysis and Detection of Persistent High-Rate Network Attacks

Table 4.3. Normalized DWT detail-energy allocation

Category	D1	D2	D3	D4
Benign traffic	0.12	0.21	0.29	0.38
SYN flood	0.31	0.34	0.23	0.12

UDP flood	0.38	0.32	0.19	0.11
HTTP flood	0.18	0.33	0.31	0.18
Benign bulk transfer	0.14	0.24	0.28	0.34

The synthetic UDP and SYN profiles place greater proportions at finer details (D1/D2), while normal bulk transfer resembles the benign allocation. The assumed differences are not general laws of attack traffic and are sensitive to aggregation rate, chosen wavelet and attack construction. Entropy derived from these fractions is similar for some categories, reinforcing the need for combined features and validation against held-out sessions.

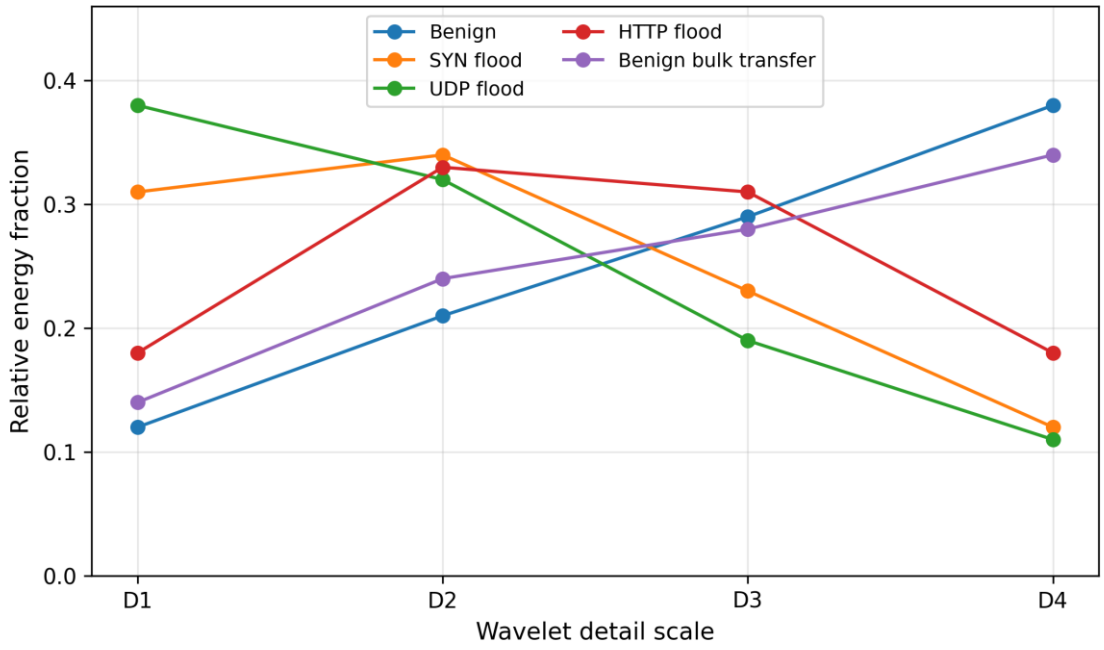


Figure 4.2. Multiscale energy profiles (constructed wavelet energy allocations).

4.3. Comparative Evaluation of AMW-TDA Against Conventional and Learning-Based Detectors

Table 4.4. Classification metrics

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	FPR (%)
Fixed threshold	91.05	91.51	90.50	91.00	8.40
DWT threshold	93.25	93.91	92.50	93.20	6.00
Random Forest	95.35	96.04	94.60	95.31	3.90
XGBoost	96.25	96.86	95.60	96.23	3.10
LSTM	95.83	96.50	95.10	95.79	3.45
AMW-TDA	97.15	97.77	96.50	97.13	2.20

Table 4.5. Confusion counts; 10,000 positives and 10,000 negatives per method

Method	TP	FN	FP	TN
Fixed threshold	9050	950	840	9160
DWT threshold	9250	750	600	9400
Random Forest	9460	540	390	9610
XGBoost	9560	440	310	9690
LSTM	9510	490	345	9655
AMW-TDA	9650	350	220	9780

The tables yield higher numerical AMW-TDA performance by design. For example, its 97.15% accuracy exceeds XGBoost by 0.90 percentage points.

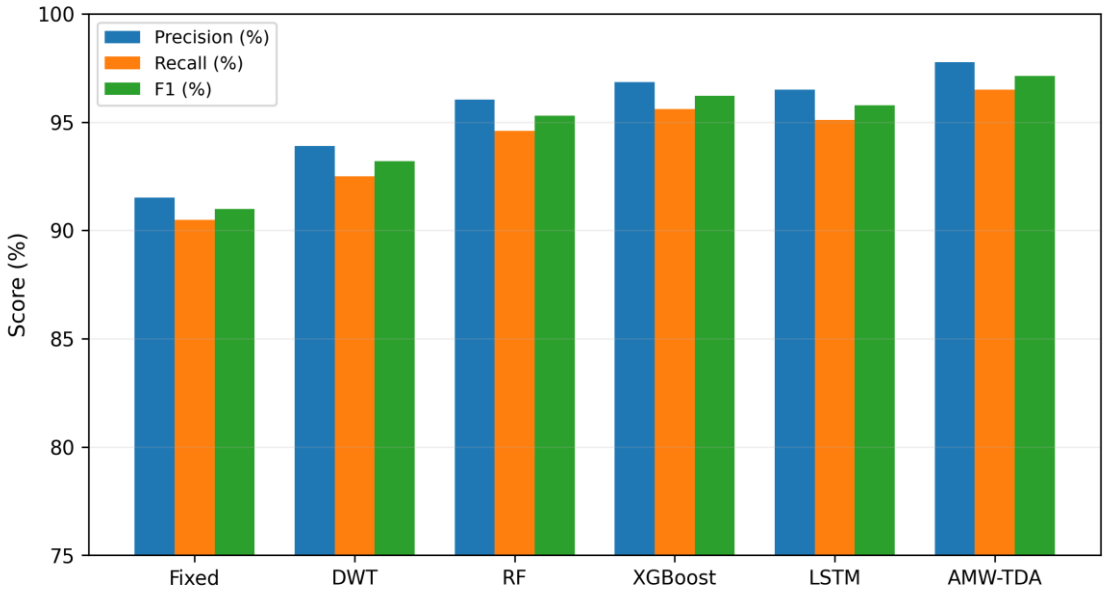


Figure 4.3. Comparative precision, recall and F1-score from constructed confusion counts.

Table 4.6. AMW-TDA ablation progression

Configuration	TP / 10,000	FP / 10,000	Recall (%)	FPR (%)
DWT only	9250	600	92.50	6.00
DWT + adaptation	9380	445	93.80	4.45
+ feature fusion	9550	310	95.50	3.10
Full persistence model	9650	220	96.50	2.20

The ablation shows the reporting structure needed to attribute gains to algorithm components. Actual results must also report additional decision delay and sensitivity to short-duration attacks caused by persistence filtering.

4.4. Real-Time Latency, Computation, Energy Consumption, and Scalability

Table 4.7. Attack-to-alert delay (ms) by load

Algorithm	10%	25%	50%	75%	90%
Fixed threshold	12	13	16	20	28
DWT threshold	17	19	24	37	64
Random Forest	22	25	33	52	84
XGBoost	26	30	39	61	100
LSTM	32	38	52	78	131
AMW-TDA	24	28	36	55	91

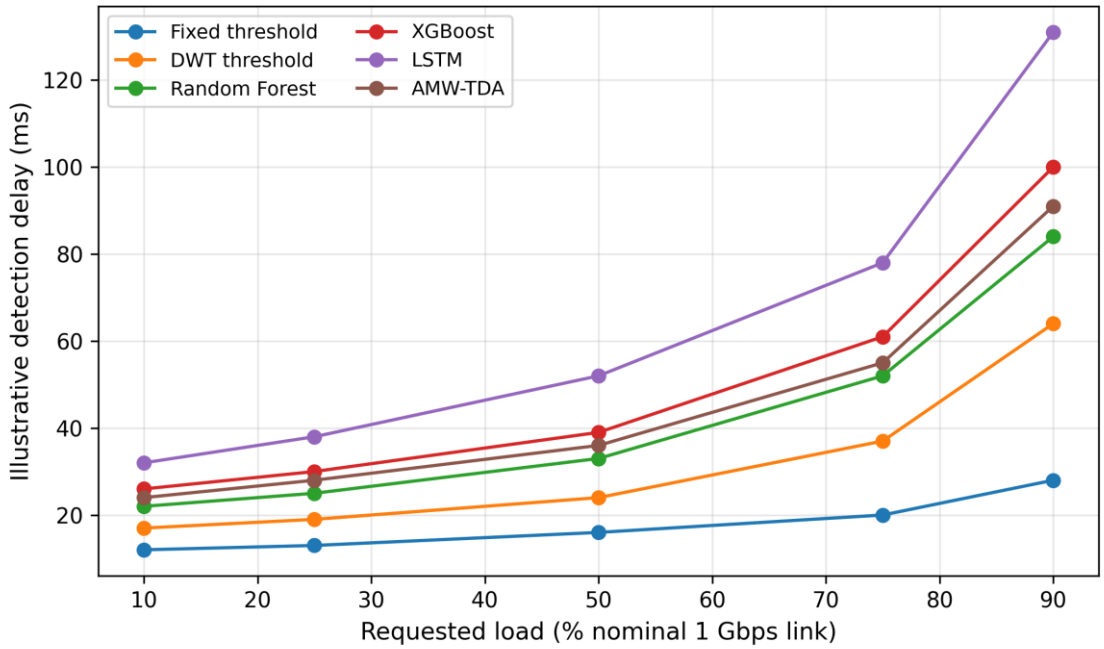


Figure 4.4. Detection latency as network loading increases; no hardware tests were performed.

$$\eta_E = \frac{8P}{R} \quad (46)$$

For steady operation ηE is joules per decimal GB when P is watts and R is gigabits per second. This relation must be evaluated with simultaneous measured power and processed throughput.

Table 4.8. Constructed energy and processing efficiency

Load (%)	Processed (Mbps)	Power (W)	Energy (J/GB)	Efficiency (%)
10	100	12.1	968.0	100.0
25	249	13.5	433.7	99.6
50	493	16.2	262.9	98.6
75	720	19.4	215.6	96.0

90	815	22.8	223.8	90.56

Table 4.9. Summary and evidence outstanding

Metric	numerical value	Evidence still required
Peak processed throughput	815 Mbps	Prototype run with capture counters
AMW-TDA accuracy	97.15%	Held-out test predictions
AMW-TDA recall	96.50%	Independent attack sessions
AMW-TDA F1	97.13%	Verified confusion matrix
AMW-TDA FPR	2.20%	Independent benign traces
Delay at 90% load	91 ms	Attack onset/alert timestamps
Max example power	22.8 W	Calibrated electrical meter
Max example temperature	61 °C	Thermal instrumentation

5. CONCLUSIONS AND RECOMMENDATIONS

5.1. Conclusions on the Design, Development, and Experimental Performance of the Device

The paper adopts the Wavelet-Based 5G Traffic Monitoring and Network Security Device, referenced in the invention documentation as UK Registered Design No. 6516712, as the structural foundation for an edge-level security monitor. Its documented elements include a compact enclosure, antenna structures, network ports, embedded analysis concept, local indicators and external reporting. The modelling and test protocol show how acquisition rate, capture loss, processing throughput, thermal load, power and decision latency must be evaluated jointly.

5.2. Conclusions on the Detection Accuracy, Computational Efficiency, and Real-Time Performance of AMW-TDA

The proposed AMW-TDA unifies DWT energy, entropy and variance features with trusted benign baseline updates, adaptive anomaly scoring and persistence-aware decisions. The mathematical framework is testable and permits controlled investigation of accuracy, false alarms, delay and resource cost. The significance of the approach will be established only if grouped independent session evaluations and algorithm ablations demonstrate a reproducible advantage. Persistence filtering must be assessed for both suppression of isolated benign bursts and possible penalties for short or low-intensity attacks.

5.3. Recommendations for Practical Deployment in 5G Telecommunications Infrastructure

Operational deployment should complement traffic anomaly analytics with authenticated configuration, controlled administrative access and protected storage. Nwatuzie et al. (2025) investigate hybrid cryptographic protection for cloud-storage integrity, while Idika and Ijiga (2025) review tamper-resistant intrusion-detection mechanisms for decentralized information exchange. These works inform device-log protection and management architecture.

First, fabricate and characterize the physical design; record the processor, interface controllers, antenna/RF receiver configuration, RAM, cooling, power supply, firmware and device revision. Second, evaluate the detector with 5G-NIDD, independent benign scenarios and distinct attack sessions under a transparent

partitioning scheme. Third, implement passive authorized mirroring in an isolated testbed before considering operational installations.

Predefine acceptance criteria for sustainable traffic load, packet capture loss, attack-to-alert delay, false-alarm rate, memory and power demand. Protect device logs, update channels, access controls and benign model calibration. Finally, compare total operational cost and detection quality against established monitoring appliances and open-source alternatives before making deployment recommendations.

5.4. Future Research Directions for Adaptive Cybersecurity Monitoring in 5G and Emerging 6G Networks

Future work should prioritize prototype implementation, repeated and independently timed attack trials, cross-session evaluation and instrumented energy measurements. Adaptive wavelet family and depth selection could be investigated under realistic load changes, along with lightweight learning models that preserve resource efficiency.

Further studies should examine heterogeneous and low-rate attacks, previously unseen network conditions, domain adaptation and baseline-poisoning resistance. Expansion to 6G remains a prospective application rather than a demonstrated capability. The device itself requires secure boot, authenticated updates, tamper-resistant logs and reproducible maintenance practices.

REFERENCES:

1. Armah, G. D., Idoko, I. P., Adeyeye, Y. I., Enyejo, L. A., & Azonuche, T. I. (2026). Predictive modeling of cyber incident escalation risk in hospital electronic medical record (EMR) systems using ensemble learning models. International Journal of Innovative Science and Research Technology, 11(2), 1312–1347. https://doi.org/10.38124/ijisrt/26feb578
2. Ayoola, V. B., James, U. U., Idoko, I. P., Ijiga, O. M., & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global Journal of Engineering and Technology Advances, 20(3), 94–117. https://doi.org/10.30574/gjeta.2024.20.3.0164
3. Balogun, S. A., Ijiga, O. M., Okika, N., Enyejo, L. A., & Agbo, O. J. (2025). Machine learning-based detection of SQL injection and data exfiltration through behavioral profiling of relational query patterns. International Journal of Innovative Science and Research Technology, 10(8). https://doi.org/10.38124/ijisrt/25aug324
4. Canadian Institute for Cybersecurity. (2019). CIC-DDoS2019 dataset. University of New Brunswick. https://www.unb.ca/cic/datasets/ddos-2019.html
5. Gabla, E. S., Peter-Anyebe, A. C., & Ijiga, O. M. (2025). Assessing machine learning enabled anomaly detection models for real time cyberattack mitigation in optical fiber communication systems. World Journal of Advanced Engineering Technology and Sciences, 17(2), 1–17. https://doi.org/10.30574/wjaets.2025.17.2.1454
6. Hoque, S., Aydeger, A., Zeydan, E., & Liyanage, M. (2025). A survey on distributed denial-of-service attack mitigation for 5G and beyond. IEEE Open Journal of the Communications Society, 6, 5840–5879. https://doi.org/10.1109/OJCOMS.2025.3586199
7. Idika, C. N., & Ijiga, O. M. (2025). Blockchain-based intrusion detection techniques for securing decentralized healthcare information exchange networks. Information Management and Computer Science, 8(2), 28–39. https://doi.org/10.26480/imcs.02.2025.28.39

8. Idika, C. N., Enyejo, J. O., Ijiga, O. M., & Okika, N. (2025). Entrepreneurial innovations in AI-driven anomaly detection for software-defined networking in critical infrastructure security. International Journal of Social Science and Humanities Research, 13(3), 150–166. https://doi.org/10.5281/zenodo.16408773
9. Idoko, I. P., Ijiga, O. M., Agbo, D. O., Abutu, E. P., Ezebuka, C. I., & Umama, E. E. (2024). Comparative analysis of Internet of Things (IoT) implementation: A case study of Ghana and the USA—vision, architectural elements, and future directions. World Journal of Advanced Engineering Technology and Sciences, 11(1), 180–199. https://doi.org/10.30574/wjaets.2024.11.1.0035
10. Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B., & Okolo, J. N. (2025). Integrating behavioral science and cyber threat intelligence (CTI) to counter advanced persistent threats (APTs) and reduce human-enabled security breaches. International Journal of Scientific Research and Modern Technology, 4(3), 1–15. https://doi.org/10.38124/ijsrmt.v4i3.376
11. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. Open Access Research Journal of Science and Technology, 11(1), 1–24. https://doi.org/10.53022/oarjst.2024.11.1.0060
12. Ijiga, O. M., Okika, N., Balogun, S. A., Enyejo, L. A., & Agbo, O. J. (2025a). A comprehensive review of federated learning architectures for insider threat detection in distributed SQL-based enterprise environments. International Journal of Innovative Science and Research Technology, 10(7). https://doi.org/10.38124/ijisrt/25jul392
13. James, U. U., Ijiga, O. M., & Enyejo, L. A. (2025). Zero trust network access enforcement for securing multi-slice architectures in 5G private enterprise deployments. International Journal of Innovative Science and Research Technology, 10(8). https://doi.org/10.38124/ijisrt/25aug323
14. Nwatuzie, G. A., Ijiga, O. M., Idoko, I. P., Enyejo, L. A., & Ali, E. O. (2025). Design and evaluation of a user-centric cryptographic model leveraging hybrid algorithms for secure cloud storage and data integrity. American Journal of Innovation in Science and Engineering, 4(2), 49–65. https://doi.org/10.54536/ajise.v4i2.4482
15. Okika, N., Nwatuzie, G. A., Odozor, L., Oni, O., & Idoko, I. P. (2025). Addressing IoT-driven cybersecurity risks in critical infrastructure to safeguard public utilities and prevent large-scale service disruptions. International Journal of Innovative Science and Research Technology, 10(2), 1333–1350. https://doi.org/10.5281/zenodo.14964285
16. Onuh, J. E., Idoko, I. P., Igbede, M. A., Olajide, F. I., Ukaegbu, C., & Olatunde, T. I. (2024). Harnessing synergy between biomedical and electrical engineering: A comparative analysis of healthcare advancement in Nigeria and the USA. World Journal of Advanced Engineering Technology and Sciences, 11(2), 628–649. https://doi.org/10.30574/wjaets.2024.11.2.0152
17. Samarakoon, S., Siriwardhana, Y., Porambage, P., Liyanage, M., Chang, S.-Y., Kim, J., Kim, J., & Ylianttila, M. (2022). 5G-NIDD: A comprehensive network intrusion detection dataset generated over 5G wireless network [Data set]. IEEE DataPort. https://doi.org/10.21227/xtep-hv36
18. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

19. Siriwardhana, Y., Samarakoon, S., Porambage, P., Liyanage, M., Chang, S.-Y., Kim, J., Kim, J., & Ylianttila, M. (2025). Descriptor: 5G wireless network intrusion detection dataset (5G-NIDD). IEEE Data Descriptions, 2, 358–369. https://doi.org/10.1109/IEEEDATA.2025.3592888
20. Ugoaghalam Uche James & Agbo James Ogboji. (2025). Network Monitoring and Security Device [Supplied invention technical documentation; identifies United Kingdom Registered Design No. 6516712].
21. Wang, K., Fu, Y., Duan, X., & Liu, T. (2024). Detection and mitigation of DDoS attacks based on multi-dimensional characteristics in SDN. Scientific Reports, 14, Article 16421. https://doi.org/10.1038/s41598-024-66907-z
22. Wang, X., Tang, D., Feng, Y., Qin, Z., Xiong, B., & Liu, Y. (2024). An LDoS attack detection method based on FSWT time–frequency distribution. Expert Systems with Applications, Article 125006. https://doi.org/10.1016/j.eswa.2024.125006