Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (Print) | 2583-7907 (Online)
Journal Homepage: https://ajcst.co/
DOI: https://doi.org/10.70112/ajcst-2026.15.1.4415

Research Article

Embedded Wireless Context-Aware Intrusion Detection for Edge Networks: An Adaptive Architecture

Bright Gazie Akwaronwu[1*], Ajaegbu Chigozirim[2], Adediran Oluwaseyi Segun[3] and Bamikole Olarewaju Aina[4]
[1,2,3,4]Department of Information Technology, Babcock University, Ilishan-Remo, Nigeria

Article Information

Article History
Received: 5 February 2026
Revised: 6 March 2026
Accepted: 25 March 2026
Published online: 5 April 2026

Keywords
Anomaly Detection
Behavioral Analysis
Context-Aware Security
Edge Computing
Internet of Things
Intrusion Detection System Temporal Feature Engineering

Correspondence*
akwaronwu0329@pg.babcock.edu.ng

ORCID
Bright Gazie Akwaronwu
https://orcid.org/0009-0004-5903-0877
Ajaegbu Chigozirim
https://orcid.org/0000-0003-1898-010X
Adediran Oluwaseyi Segun
https://orcid.org/0009-0002-3122-3103
Bamikole Olarewaju Aina
https://orcid.org/0009-0003-6507-5548

Abstract

The growth of Internet of Things (IoT) deployments has intensified security challenges in resource-constrained edge environments. This study presents an Embedded Wireless Context-Aware Intrusion Detection System (EWCA-IDS) that integrates contextual feature engineering with a fused ensemble learning framework to enhance intrusion detection reliability. The proposed architecture embeds temporal encodings, cumulative behavioral features, and contextual interactions into the detection pipeline and employs an optimized XGBoost-based fused engine to generate a unified anomaly confidence score. Experimental results using the TON_IoT dataset demonstrate strong detection performance, achieving an overall accuracy of 0.98, an ROC–AUC of 0.9975, and a high attack recall of 0.99, indicating effective detection of malicious activity with low false-negative rates. The distributional and temporal analyses demonstrate clear class separability and stable anomaly score behavior, while feature importance and correlation results indicate the influence of contextual and aggregated features. These findings support the robustness, interpretability, and suitability of the proposed intrusion detection framework beyond conventional metric-centric approaches. Further studies will focus on integrating adaptive, lightweight online learning to address evolving attack patterns in real-time edge deployments.

I. INTRODUCTION

A. Background of the Study

Internet of Things (IoT) has transformed modern electronic devices and physical assets into a seamlessly interconnected network across industrial, healthcare, transportation, and domestic environments, necessitating a paradigm shift toward edge network computing to meet demands for low latency and high bandwidth efficiency [1]. These devices are often aided by sensors and actuators to communicate through embedded wireless networks using low-power technologies such as Wireless Fidelity (Wi-Fi), ZigBee, Bluetooth Low Energy (BLE) and it likes, as depicted in Figure 1 [2], [3]. The rapid integration of these wireless systems has significantly expanded the digital ecosystem, which allow continuous data collection, processing and decision-making in real-time [4]. These network systems introduce complex security and privacy vulnerabilities caused by scalability and heterogeneity of IoT networks and it demands advanced protection mechanisms. This makes IoT edge environments highly susceptible to attacks that can compromise the reliability and safety of distributed applications [5], [6], [7].

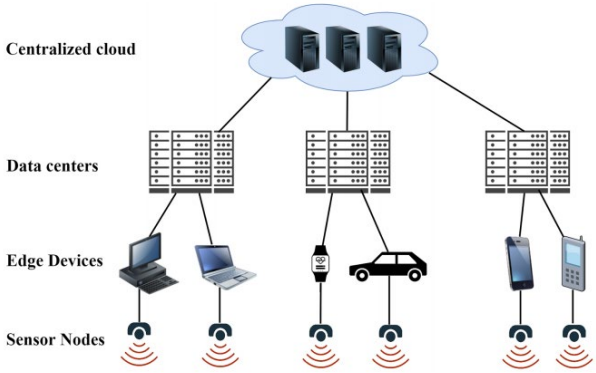

Fig.1 IoT Edge Computing Network System [8]

Recent hybrid frameworks combining machine learning and adaptive kernels demonstrate improved detection accuracy and energy efficiency in wireless networks [9], [10]. Despite these advances, achieving secure, real-time intrusion detection at the embedded edge remains challenging due to the trade-off between computational efficiency, detection precision, and energy sustainability [11], [12]. These constraints underscore the need for an embedded, context-aware intrusion detection architecture capable of operating autonomously within dynamic IoT edge environments.

Predefined rule-based IDS frameworks fail to adapt to the dynamic and heterogeneous nature of IoT systems due to their static and context-insensitive design [13], [14]. Context-aware computing introduces an adaptive dimension to network defense by allowing systems to interpret environmental and operational parameters like device behavior, network conditions, signal variations, temporal factors, and adjust their detection mechanisms accordingly [15], [16]. By incorporating contextual intelligence, IDS models can minimize false alarms, reduce redundant computations, and maintain performance stability under fluctuating network conditions. Embedded machine learning have made it feasible to integrate such adaptive intelligence directly into IoT nodes, resulting in localized, energy-efficient, and autonomous intrusion detection capabilities [17], [18], [19].

An Embedded Wireless Context-Aware Intrusion Detection System (EWCA-IDS) leverages local sensing and advanced ensemble analytics to identify abnormal network behavior in real time [20]. This approach prioritizes optimal detection performance through deep contextual intelligence while maintaining an architecture feasible for edge deployment, which align with the broader vision of secure, decentralized, and self-sustaining IoT ecosystems, where detection and response mechanisms are distributed across edge layers rather than concentrated in cloud infrastructures [21], [22]. The study aims to achieve high and reliable detection accuracy through advanced contextual feature engineering and ensemble learning. It contributes to the advancement of secure edge architectures and provides a scalable and intelligent defense mechanism that strengthens trust, resilience, and performance in next-generation IoT ecosystems.

II. METHODOLOGY

A. Method and Design

To achieve this, the study adopts a design pathway that brings together embedded sensing, context interpretation, lightweight machine learning, and adaptive decision-making as a multi-stage operational EWCA-IDS architecture in Figure 2. The model is organized into three sequential stages: Sensing and Acquisition, Contextual and Adaptive Detection, Decision, Response and Self-Tuning Layer. Each stage performs a specific function within the overall method, ensuring that raw wireless signals and device readings are gradually refined into meaningful indicators that can support accurate anomaly detection. The final stages of the method focus on local decision-making and iterative refinement, allowing the system to improve its behaviour over time. By organizing the EWCA-IDS in this structured manner, the methodology provides a clear foundation for examining how context-awareness and adaptive learning contribute to improved intrusion-detection performance in wireless edge networks.

1. Sensor and Acquisition Layer: The Edge and Communication Layer form the foundational level of the system architecture, focusing on the physical collection of data and the secure, energy-efficient transmission of information within the constrained IoT environment. Collection of raw physical data such as temperature, pressure, and other environmental metrics is initiated by the IoT Sensors which generate network traffic and act as both the primary targets and sources of data for the Intrusion Detection System (IDS). It captures network-related parameters (such as packet rate, latency, and jitter), device-level metrics (including energy level, CPU load, and memory usage), and environmental factors (such as Received Signal Strength Indicator (RSSI), node mobility, and temporal variations).

To facilitate communication, the Wireless Communication Module (WCM) ensures secure and energy-aware data exchange through protocols like ZigBee, LoRa, and Bluetooth Low Energy (BLE). This section is followed by the Edge Gateway that acts as a more powerful intermediary device positioned at the network boundary. It aggregates data from multiple nodes, manages local processing, and serves as the interface between the sensing layer and decision-making layers.

2. Contextual Processing and Adaptive Detection Layer: The Contextual Processing and Adaptive Detection Layer is raw sensory and network data are refined into meaningful context to power adaptive intrusion detection. It combines contextual interpretation, feature engineering, and machine learning–based anomaly analysis to deliver intelligent, real-time threat detection. The process begins with Feature Extraction and Normalization, which converts raw traffic and contextual metrics into a structured dataset through encoding and dimensionality reduction. It prepares the data for deeper

contextual understanding by the Context Modeling Engine, which interprets system states using semantic representations to derive descriptive variables such as High Load, Low Energy, or Normal Operation.

At the detection stage, the Embedded Adaptive IDS Engine employs an ensemble learning model**,** to evaluate anomalies in real time. This model serves as the fused decision engine, leveraging the multi-dimensional contextual features to achieve superior discriminative power and minimize false alarms.

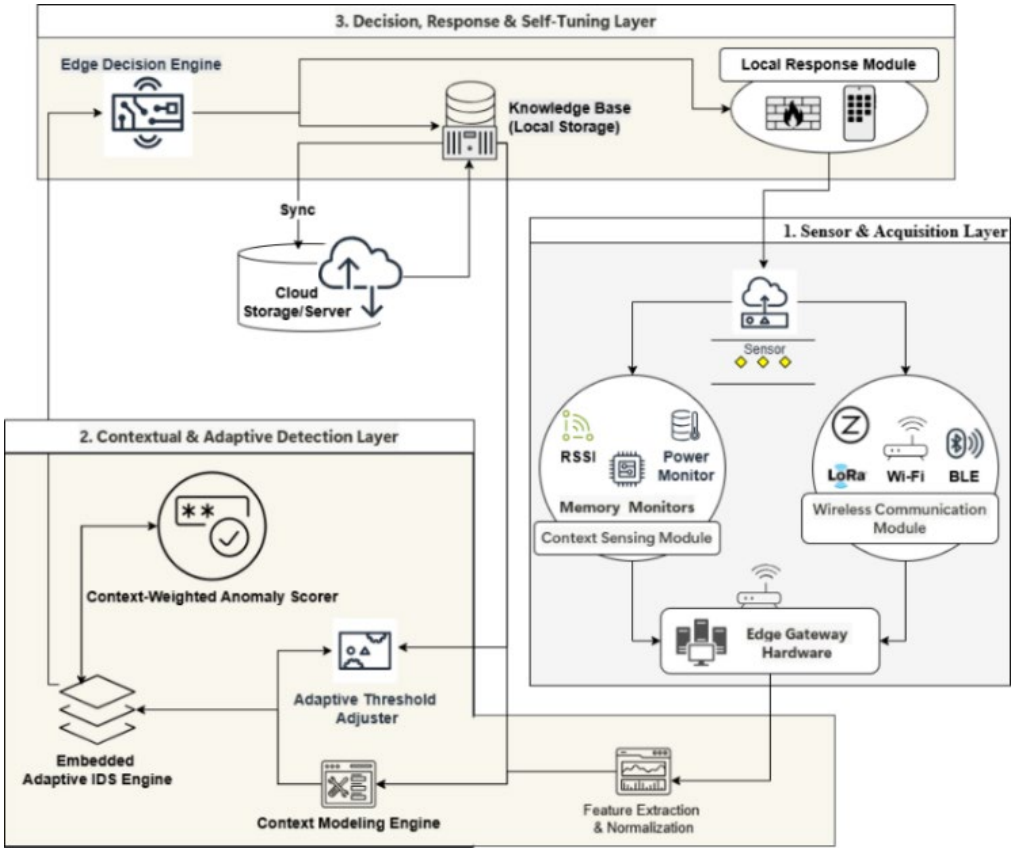

Fig.2 EWCA-IDS Architectural Framework

3. Decision, Response & Self-Tuning Layer: The Decision, Response, and Self-Tuning Layer is responsible for finalizing intrusion decisions, coordinating rapid countermeasures and sustaining long-term adaptability. It integrates decision intelligence, local mitigation and feedback-driven learning to ensure continuous operational resilience. The Edge Decision Engine aggregates anomaly indicators and detection alerts from multiple nodes, applying consensus analysis to derive the final intrusion classification with an associated confidence level. Once a threat is confirmed, the Local Response Module executes targeted mitigation strategies at the edge, such as isolating compromised nodes, rate-limiting abnormal traffic, or securely exchanging alerts with neighboring gateways.

To support continual learning, the Adaptive Feedback Loop updates a centralized knowledge base that records contextual interactions, response outcomes, and behavioral profiles, enabling ongoing system refinement based on decision results. This mechanism provides real-time input to components such as the Context-Weighted Anomaly Scorer and Adaptive Threshold Adjuster, enabling self-tuning and sustained accuracy against dynamic and evolving threat landscapes.

B. EWCA-IDS Experimental Validation Pipeline

To evaluate the performance and adaptive capabilities of the proposed EWCA-IDS architecture, a five-stage Validation Pipeline (Figure 3) using the TON_IoT dataset [23] is designed to isolate and measure the impact of the context-aware components (Context Modeling Engine and Adaptive Threshold Adjuster) on detection accuracy and false positive rates.

The pipeline is structured sequentially, ensuring that each stage builds upon the outputs of the previous one, culminating in a comparative performance analysis. Each stage is aligned with a corresponding architectural layer and producing distinct analytical outputs that feeds another stage(s). The first stage, Data Acquisition and Preprocessing, corresponds to the Edge and Communication Layer where the dataset is obtained, cleaned, and preprocessed and partitioning the data into training, validation, and testing subsets. It is followed by the Contextual Feature Engineering,

aligns with the *Contextual Processing Layer*, where the Context Modeling Engine is employed to translate raw metrics into high-level contextual variables, resulting in a fused feature set that integrates both network and contextual dimensions alongside defined context mapping rules.

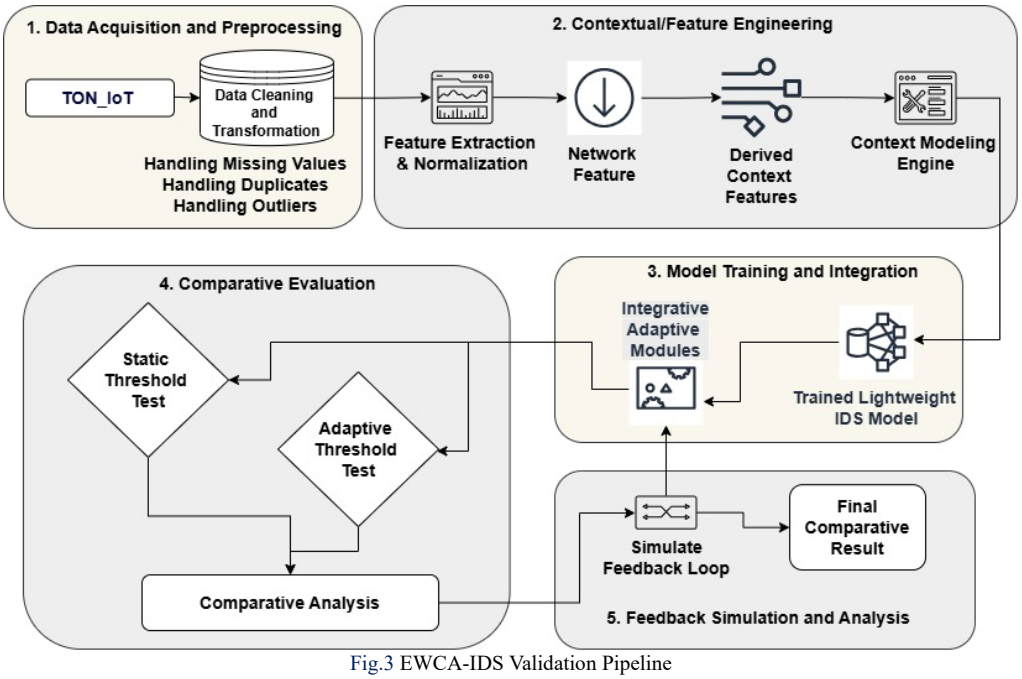

Fig.3 EWCA-IDS Validation Pipeline

The Model Training and Integration follows within the Adaptive Detection Layer. This stage involves class balancing using SMOTE and training the dataset with a robust Extreme Gradient Boosting (XGBoost) ensemble model. The model serves as the fused EWCA-IDS engine, replacing the original distance-based anomaly scorer. The Feedback Loop Simulation and Analysis stage corresponds to the Self-Tuning Feedback Layer. This phase models the Adaptive Feedback Loop, which represents the system's ability to iteratively refine its learning parameters and decision logic based on observed outcomes. The analysis highlights the system's capacity for self-tuning and sustained stability over time, yielding the final comparative performance results.

C. Algorithmic Framework and Learning Strategy

The EWCA-IDS operates based on an adaptive, context-driven learning framework designed to detect anomalous behaviors in IoT edge networks while minimizing false alarms and computational costs. The algorithm integrates statistical profiling, context-weighted learning, and threshold adaptation to enable real-time, localized intrusion detection across distributed embedded nodes. Each IoT node n_i continuously collects a set of contextual attributes $X_i = \{x_{i1}, x_{i2}, \dots, x_{im}\}$, representing measurable parameters which include raw sensor data, cyclical temporal state (encoded as sine/cosine), behavioral lag features, rate-of-change metrics, and feature interaction terms. This multi-dimensional feature set is the foundation of the Context Modeling Engine. These parameters form a multi-dimensional context vector, (1) and each parameter is normalized using min–max scaling (2),

$$X_{\mathbf{i}}(t) = [x_{i1}(t), x_{i2}(t), \dots, x_{im}(t)] \in R^d, \quad \dots (1)$$

$$\tilde{X}_{ij}(t) = \frac{x_{ij}(t) - \min(x_j)}{\max(x_j) - \min(x_j)} \quad \dots (2)$$

This normalization ensures feature uniformity and enables the IDS to compare heterogeneous attributes under varying operational conditions. The resulting normalized feature vectors define a unified contextual feature space that serves as the input to the detection model. To achieve robust and highly discriminative intrusion detection within the constraints of IoT edge environments, the EWCA-IDS adopts an ensemble learning strategy based on XGBoost as its core classification engine, operating over this combined network and contextual feature space. Accordingly, let $d$denote the dimensionality of the feature space produced by the Context Modeling Engine. Given a training dataset $\mathcal{D} = \{(\mathbf{x}_{ij}, y_i)\}_{i=1}^{N}$, where $y_i \in \{0,1\}$ denotes normal or attack traffic, XGBoost models the prediction as an additive ensemble of decision trees (3).

$$y = \sum_{k=1}^{K} f_k(x_i), \ f_x \in F, \dots (3)$$

where each f_k represents a regression tree in the functional space $\mathcal{F}$, and K is the total number of trees in the ensemble. The model parameters are learned by minimizing the regularized objective function (4).

$$L = \sum_{i=1}^{N} \ell(y_i, \hat{y}_i), + \sum_{k=1}^{K} \Omega(f_k), \ldots (4)$$

where $\ell(\cdot)$ is the classification loss (logarithmic loss in this study) and $\Omega(f_k)$ is a regularization term that penalizes model complexity to prevent overfitting. This formulation enables EWCA-IDS to learn stable yet expressive decision boundaries that are resilient to noisy and dynamically evolving IoT traffic patterns.

To ensure that this learning strategy are implemented and to mitigate classifier bias toward the majority class and improve sensitivity to rare intrusion events, the Synthetic Minority Over-sampling Technique (SMOTE) is applied exclusively to the training dataset. Given a minority-class (x_i), SMOTE generate a synthetic instance $\mathbf{x}_{\text{new}}$ as seen in (5)

$$\mathbf{x}_{\text{new}} = \mathbf{x}_i + \lambda(\mathbf{x}_{\text{nn}} - \mathbf{x}_i), \qquad \lambda \in (0,1), \ldots (5)$$

where $\mathbf{x}_{\text{nn}}$ is one of the k-nearest neighbors of $\mathbf{x}_i$ in feature space.

Applying SMOTE prior to ensemble training ensures that the XGBoost classifier is exposed to a balanced representation of normal and attack traffic, thereby maximizing recall for intrusion classes, which is critical for security-sensitive IoT deployments where false negatives are costly. After class balancing, the XGBoost ensemble is trained on the resampled dataset, forming the final fused EWCA-IDS engine. The trained model outputs an intrusion probability score that feeds into the context-weighted scoring and adaptive threshold mechanisms described in subsequent sections. Experimental results demonstrate that this combined ensemble learning and class-balancing strategy yields near-perfect discriminative performance, confirming its effectiveness for real-time, edge-based intrusion detection.

D. Model Evaluation

To assess the effectiveness of the proposed EWCA-IDS, several performance metrics were selected to capture both detection accuracy and operational efficiency within an IoT edge environment. Given the complexity of the multi-component fusion, a highly optimized XGBoost ensemble model is used as the final fused decision engine, providing a robust upper bound on the system's discriminative capacity. The primary classification metrics include accuracy, which reflects the overall proportion of correctly identified traffic instances, and precision and recall, which respectively measure the system's ability to avoid false alarms and its sensitivity to true attack events. The F1-score, representing the harmonic mean of precision and recall, provides a balanced indicator of classification quality under imbalanced traffic conditions common in IoT networks.

In addition to these metrics, the false positive rate (FPR) is reported to show how effectively the context-aware mechanism minimizes incorrect anomaly flags. Detection latency is measured to evaluate how quickly the system identifies malicious behavior, a crucial factor for time-sensitive applications at the edge. Energy consumption and computational overhead are included to quantify the feasibility of deploying the IDS on embedded devices with constrained resources. Finally, where applicable, Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) scores are used to illustrate the model's discriminative capability across varying threshold settings. Together, these metrics provide a comprehensive assessment of EWCA-IDS in terms of accuracy, responsiveness, robustness, and practical deplorability.

III. RESULTS AND DISCUSSION

This section presents a comprehensive evaluation and critical discussion of the proposed Embedded Wireless Context-Aware Intrusion Detection System (EWCA-IDS). The analysis is designed to assess the detection effectiveness, robustness and adaptive behavior within a realistic IoT edge computing context, and it examines both quantitative performance metrics and qualitative behavioral characteristics of the EWCA-IDS. Further analyses investigate the distributional and temporal behavior of EWCA-fusion anomaly scores, the contribution and interaction of contextual features, and the system's adaptive response around representative attack events.

The model produces a continuous anomaly confidence score, referred to as the EWCA-fusion anomaly score. Performance evaluation employed a comprehensive set of metrics to assess both detection effectiveness and operational reliability in an IoT edge context, including accuracy, precision, recall, F1-score, false positive rate, and threshold-independent measures such as ROC curves and AUC, complemented by visualization-driven analyses to examine error characteristics and score behavior. The classification outcomes of the proposed EWCA-IDS using quantitative evaluation results obtained on the test dataset is summarized in Table I.

TABLE I EWCA-IDS CLASSIFICATION PERFORMANCE

Metric	Class 0 (Normal)	Class 1 (Attack)	Overall
Precision	1.00	0.91	0.98
Recall	0.97	0.99	0.98
F1-score	0.98	0.95	0.98
ROC–AUC	-	-	0.9975
Accuracy	-	-	0.98

The EWCA-IDS demonstrates strong detection performance, achieving an accuracy of 0.98 and a high ROC–AUC score of 0.9975. The high recall value for attack traffic (0.99) confirms that the system is highly sensitive to intrusion events, minimizing false negatives that could pose significant security risks in IoT edge networks. The precision score of 1.00 for normal traffic indicates that benign activities are classified with very high confidence, resulting in a low false positive rate and reduced alert noise. Although the precision

for attack traffic is slightly lower (0.91), this trade-off reflects a deliberate emphasis on detection sensitivity, which is appropriate for security-critical applications.

A. Threshold-Independent and Imbalance-Aware Performance Analysis

The detection capability of EWCA-IDS is further examined using threshold-independent and imbalance-aware analyses based on the Receiver Operating Characteristic (ROC) and Precision–Recall (PR) curves. The ROC curve for EWCA-IDS exhibits a steep ascent toward the upper-left corner, yielding an ROC–AUC score of 0.9975. This indicates excellent discriminative capability, demonstrating that the EWCA-fusion detection engine can effectively distinguish between normal and attack traffic across a wide range of threshold settings. The strong ROC performance illustrated in Figure 4 confirms that the model maintains a high true positive rate while keeping false positives at a minimal level.

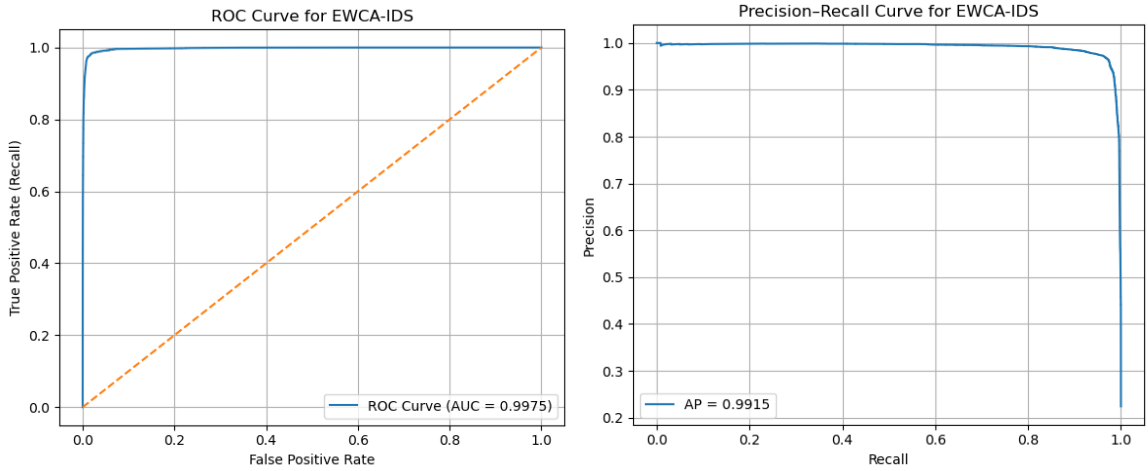

Fig.4 ROC Performance Curves

Given the imbalanced nature of the dataset, Precision–Recall analysis provides a more attack-centric evaluation of performance. The Precision–Recall curve indicates that EWCA-IDS sustains very high precision across most recall levels, with an average precision (AP) of 0.9915. This behavior confirms that the system achieves high attack detection sensitivity while maintaining acceptable false alarm rates.

B. Distributional and Temporal Behavior of EWCA-Fusion Scores

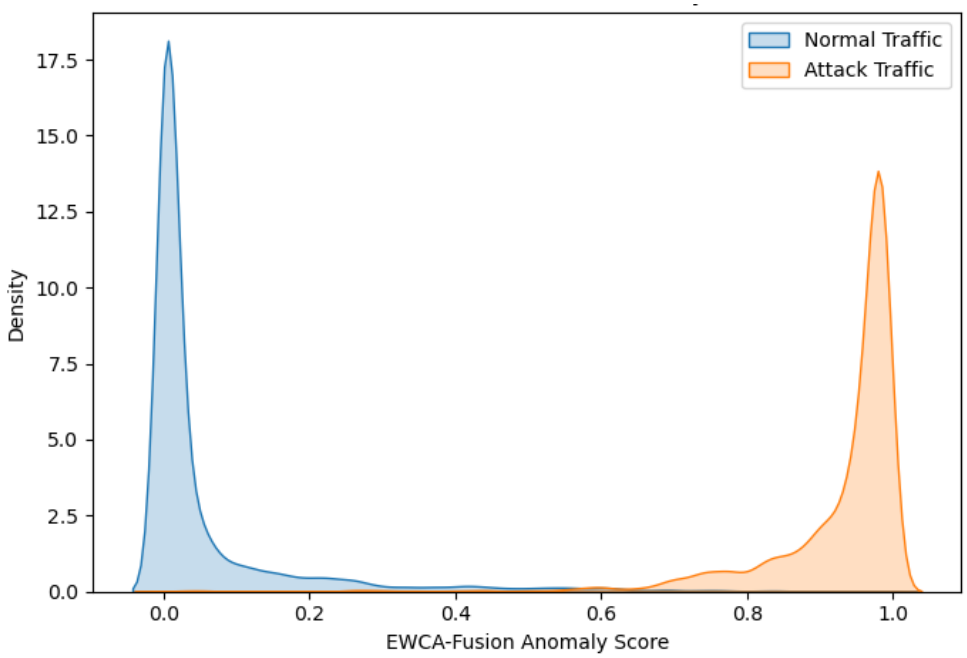

Fig.5 Distribution of EWCA-Fusion Anomaly Scores

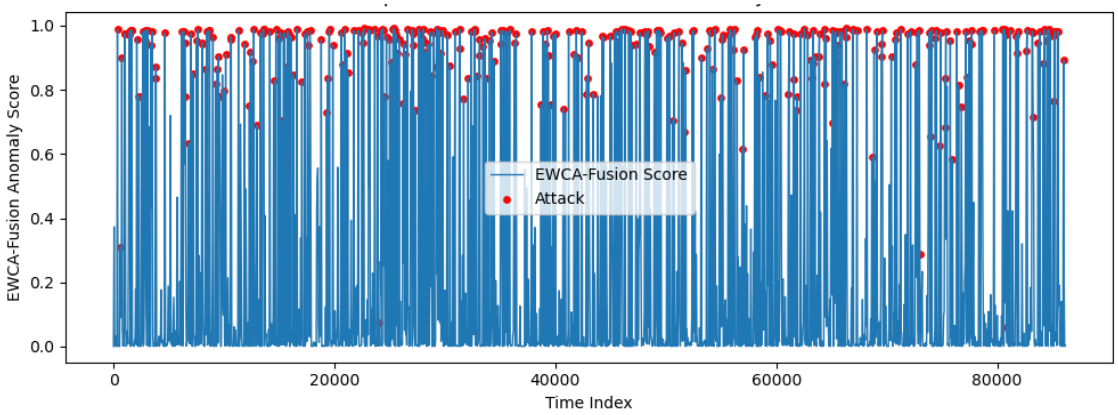

Fig.6 Temporal Behavior of EWCA-Fusion Anomaly Scores

To evaluate the practical reliability of EWCA-IDS, the study examined the distributional separability and temporal dynamics of the EWCA-fusion anomaly scores and provided an insight into how confidently the fused score distinguishes normal from attack traffic and how responsively it evolves over time under realistic operating conditions. The distribution of EWCA-fusion anomaly scores for normal and attack traffic is illustrated in Figure 5 exhibit clear separation, with normal traffic concentrated at lower anomaly score values and attack traffic clustered at significantly higher values, with minimal overlap between the two classes.

The temporal evolution of the EWCA-fusion scores is illustrated in Figure 6, with attack events explicitly marked shows stable score behaviour during benign operation, interrupted by sharp and immediate score escalations during intrusion events. This temporal alignment indicates prompt detection of malicious activity while maintaining low volatility under normal conditions**.** These analyses confirm that the EWCA-fusion anomaly score provides both reliable class separability and responsive temporal behavior, reinforcing the robustness and practical applicability of the proposed EWCA-IDS.

C. Contextual Feature Contribution and Component Interaction

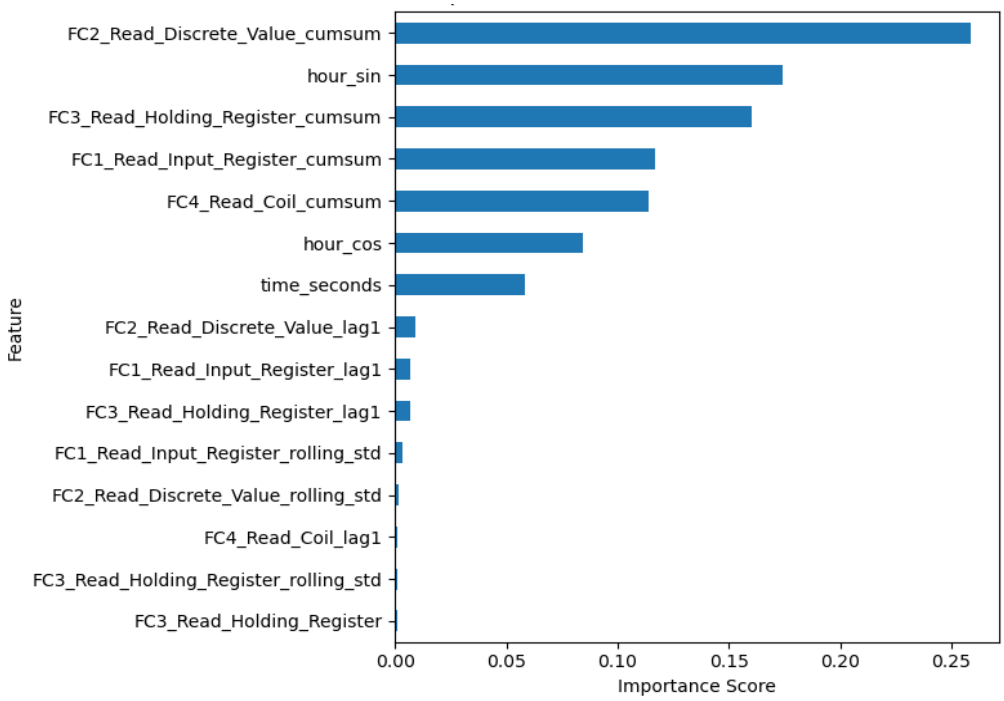

Fig.7 Top Contextual Feature Contributions in EWCA-IDS

To provide interpretability and validate the effectiveness of the proposed context-aware design, the relative contribution of contextual features and the interaction patterns among key components were analyzed within the EWCA-fusion detection engine. The EWCA-IDS decision process is dominated by contextual and temporal aggregation features, particularly cumulative Modbus register behaviors and cyclic time encodings as seen in Figure 7. In contrast, instantaneous and short-lag features contribute less to the final decision, indicating that the model prioritizes long-term behavioral context over isolated observations. This confirms the effectiveness of the proposed Context Modeling Engine in

capturing meaningful operational patterns. Component interaction is further analyzed through correlation matrices under normal and attack conditions. The normal operation inter-component correlations remain weak and stable, reflecting independent feature dynamics, while the component correlation under attack operation reveals noticeable shifts in dependency patterns, with several contextual features exhibiting stronger alignment with the EWCA-fusion anomaly score. Together, these results demonstrate that EWCA-IDS effectively leverages influential contextual features and their coordinated interactions to achieve robust and interpretable intrusion detection suitable for embedded wireless IoT edge environments.

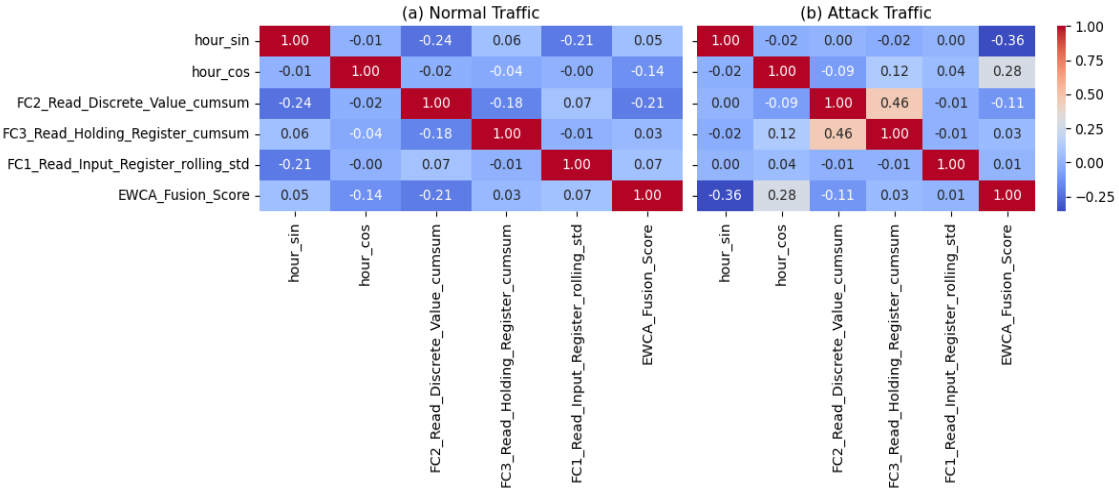

Fig.8 Composite Correlation Heatmap (Normal vs Attack)

D. Case-Based Temporal Analysis and Adaptive Detection Behavior

To conclude the results and discussion, a case-based temporal analysis is conducted to illustrate the adaptive detection behavior of the proposed EWCA-IDS around a representative attack event. Unlike the global temporal analysis presented earlier, this localized evaluation focuses on the system's real-time responsiveness and post-event stability. The EWCA-fusion anomaly score (seen in Figure 9) remains stable during normal operation and exhibits a sharp escalation immediately at the onset of the attack. This rapid increase indicates prompt detection of malicious activity, while the subsequent stabilization of the score after the event demonstrates the system's ability to adapt without prolonged alert persistence. The clear temporal alignment between the attack onset and anomaly score escalation confirms that EWCA-IDS responds to contextual disruptions in a timely and controlled manner. These characteristics collectively validate the suitability of the proposed system for reliable, real-time intrusion detection in embedded wireless IoT edge environments.

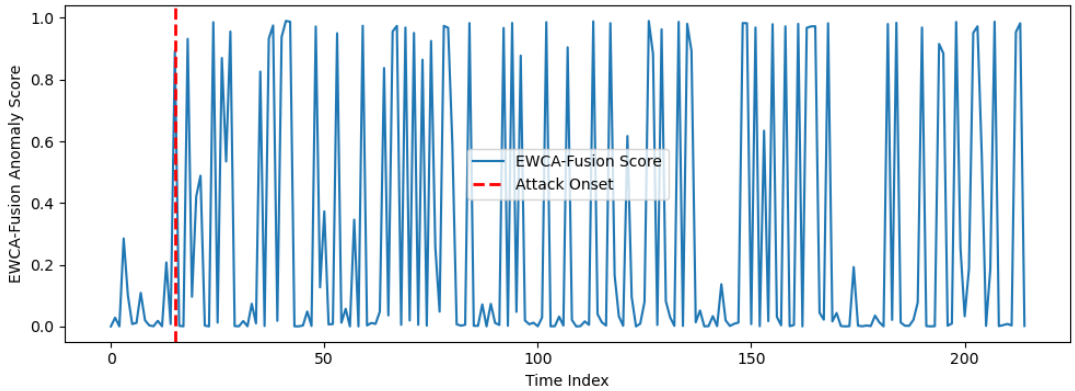

Fig.9 Case-Based Temporal Behavior of EWCA-Fusion Scores

IV. CONCLUSION AND FUTURE WORK

This study presented an Embedded Wireless Context-Aware Intrusion Detection System (EWCA-IDS) designed to address the limitations of conventional intrusion detection approaches in resource-constrained IoT edge environments. Unlike existing IDS solutions that rely primarily on instantaneous traffic features or centralized processing, the proposed framework integrates contextual feature engineering with a fused ensemble decision engine to capture both temporal behavior and cumulative network dynamics. By embedding contextual intelligence directly into the

detection pipeline, EWCA-IDS enables more reliable discrimination between benign variability and malicious activity at the edge. Comprehensive experimental evaluation demonstrated that EWCA-IDS achieves strong detection performance, robust class separability, and stable temporal behavior under realistic attack conditions. Beyond aggregate accuracy metrics, the study provided distributional, temporal, and interpretability-driven analyses, offering a deeper understanding of how contextual features and their interactions contribute to intrusion detection decisions. This multi-perspective evaluation distinguishes the proposed approach from prior IDS studies that focus primarily on classification performance without examining operational behavior or decision structure. Future work will explore adaptive thresholding mechanisms to further enhance responsiveness under evolving network conditions, extend the framework to support multi-class attack categorization, and investigate lightweight online learning strategies to accommodate long-term concept drift. Additional validation on heterogeneous IoT datasets and real-world edge deployments will further assess scalability and practical feasibility.

Declaration of Conflicting Interests
The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation
The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

REFERENCES

[1] U. Rehman *et al*., "Internet of Things in healthcare research: Trends, innovations, security considerations, challenges and future strategy," *Int. J. Intell. Syst.*, vol. 2025, no. 1, Jan. 2025, doi: 10.1155/int/8546245.

[2] M. Mansour *et al*., "Internet of Things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions," *Energies*, vol. 16, no. 8, p. 3465, Apr. 2023, doi: 10.3390/en16083465.

[3] H. N. S. Aldin, M. R. Ghods, F. Nayebipour, and M. N. Torshiz, "A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology," *Sensors Int.*, vol. 5, p. 100258, 2024, doi: 10.1016/j.sintl.2023.100258.

[4] A. I. Zreikat, Z. AlArnaout, A. Abadleh, E. Elbasi, and N. Mostafa, "The integration of the Internet of Things (IoT) applications into 5G networks: A review and analysis," *Computers*, vol. 14, no. 7, p. 250, Jun. 2025, doi: 10.3390/computers14070250.

[5] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," *J. Inf. Intell.*, vol. 2, no. 6, pp. 455–513, Nov. 2024, doi: 10.1016/j.jiixd.2023.12.001.

[6] G. Akwaronwu, I. U. Akwaronwu, and O. J. Adeniyi, "Machine learning for detecting DoS attack: A comparative approach," *Br. J. Comput. Netw. Inf. Technol.*, vol. 8, no. 2, pp. 51–70, 2025, doi: 10.52589/bjcnit-i0v0hk0y.

[7] B. G. Akwaronwu, I. U. Akwaronwu, and O. J. Adeniyi, "Brute Force Attack Detection in Network Traffic Using Convolutional Neural Networks," *Asian J. Res. Comput. Sci.*, vol. 18, no. 5, pp. 387–402, Apr. 2025, doi: 10.9734/ajrcos/2025/v18i5662.

[8] A. A. Al-Saedi, V. Boeva, E. Casalicchio, and P. Exner, "Context-aware edge-based AI models for wireless sensor networks—An overview," *Sensors*, vol. 22, no. 15, pp. 1–33, 2022, doi: 10.3390/s22155544.

[9] L. Li, Q. Zhang, X. Xiong, A. Li, and G. Chen, "A fault diagnosis and prediction method for wireless sensor networks based on attention mechanism fused neural networks," *Int. J. Commun. Syst.*, vol. 38, no. 15, Oct. 2025, doi: 10.1002/dac.70244.

[10] A. Bahadori-Jahromi, S. Room, C. Paknahad, M. Altekreeti, Z. Tariq, and H. Tahayori, "The role of artificial intelligence and machine learning in advancing civil engineering: A comprehensive review," *Appl. Sci.*, vol. 15, no. 19, p. 10499, Sep. 2025, doi: 10.3390/app151910499.

[11] H. G. A. Umar *et al*., "Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model," *J. Cloud Comput.*, vol. 14, no. 1, p. 32, 2025, doi: 10.1186/s13677-025-00762-9.

[12] Y. Huang, M. Ma, W. J. K. Raymond, and C.-O. Chow, "An adaptive intrusion detection system for the Internet of Things using large language models and post-quantum-secure blockchain," *Comput. Netw.*, p. 111819, Nov. 2025, doi: 10.1016/j.comnet.2025.111819.

[13] F. Alserhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design," *Sensors*, vol. 25, no. 15, p. 4720, Jul. 2025, doi: 10.3390/s25154720.

[14] M. N. Halgamuge and D. Niyato, "Adaptive edge security framework for dynamic IoT security policies in diverse environments," *Comput. Secur.*, vol. 148, p. 104128, Jan. 2025, doi: 10.1016/j.cose.2024.104128.

[15] Z. Noor, S. Hina, F. Hayat, and G. A. Shah, "An intelligent context-aware threat detection and response model for smart cyber-physical systems," *Internet Things*, vol. 23, 2023, doi: 10.1016/j.iot.2023.100843.

[16] J. Violos, G. Mamanis, I. Kompatsiaris, and S. Papadopoulos, "Cognition and context-aware decision-making systems for a sustainable planet: A survey on recent advancements, applications and open challenges," *Discov. Sustain.*, vol. 6, no. 1, p. 235, 2025, doi: 10.1007/s43621-025-00954-y.

[17] N. Mazhar, R. Salleh, M. A. Hossain, and M. Zeeshan, "SDN-based intrusion detection and prevention systems using manufacturer usage description: A survey," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, pp. 717–737, 2020, doi: 10.14569/IJACSA.2020.0111283.

[18] A. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discov. Artif. Intell.*, vol. 5, no. 1, p. 314, 2025, doi: 10.1007/s44163-025-00578-1.

[19] J. O. Adeyemi, S. O. Ogunlere, and B. G. Akwaronwu, "Real-Time Detection of Examination Malpractices Using Convolutional Neural Networks and Video Surveillance: A Systematic Review with Meta-Analysis," *Br. J. Comput. Netw. Inf. Technol.*, vol. 8, no. 2, pp. 15–50, May 2025, doi: 10.52589/BJCNIT-QC5EELJE.

[20] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "MetaWatch: Trends, challenges, and future of network intrusion detection in the metaverse," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 32469–32492, Aug. 2025, doi: 10.1109/JIOT.2025.3568477.

[21] U. Khan, F. M. Khan, Z. A. Haider, and F. Alturise, "Integrating AI, blockchain, and edge computing for zero-trust IoT security: A comprehensive review of advanced cybersecurity framework," *Comput. Mater. Contin.*, vol. 85, no. 3, pp. 4307–4344, 2025, doi: 10.32604/cmc.2025.070189.

[22] Singh *et al*., "A systematic review of blockchain, AI, and cloud integration for secure digital ecosystems," *Int. J. Networked Distrib. Comput.*, vol. 13, no. 2, p. 28, 2025, doi: 10.1007/s44227-025-00072-1.

[23] N. Moustafa, "The TON_IoT datasets," UNSW Canberra at ADFA, Canberra, Australia, 2021. [Online]. Available: https://research.unsw.edu.au/projects/toniot-datasets.