Dynamic attack pattern-aware intelligent cyber-physical intrusion detection system for internet of things-edge networks

Vishala Ibasapura Lakshminarayanappa[1], Kempahanumaiah M. Ravikumar[2]
[1]Department of Electronics and Communication, SJC Institute of Technology, Bangalore, India
[2]Department of Electronics and Communication, Vivekanand Institute of Technology, Bangalore, India

Article Info

Article history:

Received Jul 24, 2025
Revised Dec 26, 2025
Accepted Jan 10, 2026

Keywords:

Adaptive threat detection
Cyber-physical systems
Edge computing
Internet of things
Intrusion detection system

ABSTRACT

The proliferation of internet of things (IoT) technologies, coupled with the convergence of edge computing infrastructures, has revolutionized modern cyber-physical systems (CPS). However, the inherently distributed architecture of these systems increases their vulnerability to advanced network-level cyber threats, posing significant challenges to data integrity and system reliability. Traditional machine learning (ML) and deep learning (DL)-based intrusion detection systems (IDS) often fall short in identifying evolving attack vectors due to their limited adaptability. To address these limitations, this paper introduces a novel dynamic attack pattern-aware improvised weighted gradient boosting (DAPA-IWGB) model designed to enhance real-time threat detection and adaptive response within IoT-edge-enabled CPS environments. The DAPA-IWGB framework synergizes gradient tree boosting with an enhanced loss function handling covariate shift, while incorporating statistical monitoring mechanisms for dynamic covariate shift recognition and continuous learning. Comprehensive experimental validation using two prominent benchmark datasets ToN-IoT and UNSW-NB15 demonstrates the proposed model's robustness and superior performance, achieving detection accuracies of 99.921% and 99.93%, respectively. Comparative evaluations highlight substantial improvements in detection accuracy, adaptability, and reliability over existing IDS solutions. The results affirm the effectiveness of the DAPA-IWGB model in fortifying the security posture of distributed IoT-based CPS against sophisticated and evolving cyber threats.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Vishala Ibasapura Lakshminarayanappa
Department of Electronics and Communication, SJC Institute of Technology
Bangalore, India
Email: vishalail_12@rediffmail.com

1. INTRODUCTION

The internet of things (IoT) has emerged as a transformative paradigm, enabling real-time data exchange and intelligent decision-making through interconnected physical devices. Applications span across smart cities, industrial automation, healthcare, and vehicular networks [1], [2]. These deployments are typically supported by edge and cloud computing infrastructures to manage latency, computation, and storage limitations [3], [4]. However, highly distributed and heterogeneous nature of IoT ecosystems introduces new cybersecurity risks. Devices with limited computing power and minimal built-in security are susceptible to cyber threats such as spoofing, distributed denial of service (DDoS), and data tampering [5]–[7] as in Figure 1.

Among these, network-level attacks like link flooding, backdoors, spamming, ransomware, and DDOS are particularly dangerous, because they impair edge node availability and interfere with real-time data flows [8]–[10]. When it comes to keeping an eye out for unusual activity in these settings, intrusion detection systems (IDS) are essential [5], [11]. The dynamic traffic and changing attack patterns in IoT-edge deployments are unsuitable for traditional IDS techniques, which mostly rely on rule-based processes or static signatures [12], [13]. The use of deep learning (DL) and machine learning (ML) to enhance IDS capabilities has been the subject of recent study. ML methods analyze network traffic patterns, while DL architectures can capture deep hierarchical features from raw data [12], [14]. Despite their promise, these systems face critical limitations in detecting unseen or evolving attacks due to covariate shift where data distributions change over time [15]–[17]. Additionally, most existing IDS solutions struggle with real-time adaptation, scalability, and data imbalance, resulting in increased false positives and missed detections. Therefore, adaptive and lightweight IDS solutions tailored to edge-IoT architectures are essential for robust and scalable cyber-physical systems (CPS) security.

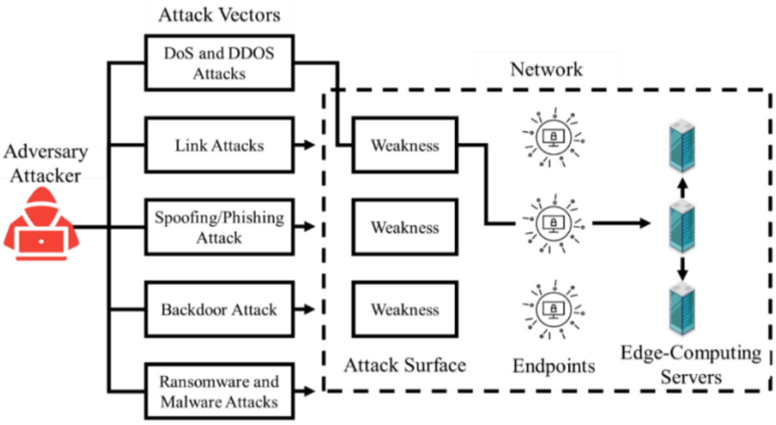

Figure 1. Basic architecture of different attacks induced in IoT-edge computing networks

The detection of intrusions in IoT networks has attracted significant research interest, with numerous studies applying intelligent learning techniques for real-time security monitoring [18]. Saiyed and Al-Anbagi [18] introduced a DDoS detection framework using genetic algorithms and statistical testing, demonstrating high precision on IoT traffic datasets. Cui *et al.* [19] proposed a deep residual network with attention mechanisms (DRN-AM) for improved detection in multi-device settings. Javeed *et al.* [20] addressed intrusion detection in smart agriculture using edge-based learning (IDS-SAEL) frameworks for hostile environments. Graph learning frameworks and federated models are gaining traction for distributed and privacy-preserving detection. Yang *et al.* [21] utilized graph-based anomaly detection to enhance link anomaly recognition (GAD-ELAR). Bouzinis *et al.* [22] introduced StatAvg, a federated learning method to address data heterogeneity in IDS. Similarly, Fares *et al.* [23] introduced ST-LSTM-DTL by integrating swin transformers (ST) and long short-term memory (LSTM) in a hybrid DL-based transfer learning (DTL) model for scalable IDS in IoT. Transfer and multi-view learning approaches have also been explored. Li *et al.* [24] performed comparative studies on single- and multi-view learning (SMVL) models, identifying benefits of diversified feature representations using auto-encoder (AE) and convolutional neural networks (CNNs). Li *et al.* [25] applied semi-supervised learning (SL) combined with random forests (RF) for intrusion detection, effectively handling partially labeled datasets.

Transformer-based models such as attack-aware divide-and-conquer transformer (TRACER) [26] and reconstruction memory network (ReMeNet) [27] have shown promise in industrial internet of things (IIoT) and transportation CPS respectively. These models excel in capturing long-range dependencies, but often require high computational resources. Bian and Liu [28] proposed a representation learning model Gaussian-mixture Cramér-wold auto-encoder (GMCWAE), achieving improved accuracy across multiple datasets. Chandnani *et al.* [29] introduced federated multi-layered deep-learning (Fed-MLDL) and achieve 98% accuracy across CICIoT, ToN-IoT, and Edge-IIoTset datasets. Elaziz *et al.* [30] proposed a federated intrusion detection framework using tab transformers and metaheuristic tuning, demonstrating effectiveness across benchmarks like N-BaIoT and CICIoT2023. While these methods show improved performance in specific contexts, many do not adequately address covariate shift, data imbalance, or real-time adaptability critical for dynamic edge-IoT settings. A recurring limitation is reliance on static models trained on fixed balanced datasets, which are unable to adapt to novel attack patterns emerging in real-world imbalanced traffic [31].

Despite extensive research in ML/DL-based IDS frameworks, existing systems often suffer from critical shortcomings when deployed in dynamic IoT-edge environments [31]. These include: i) lack of adaptability: most models are trained on static datasets and cannot respond to changes in attack behaviors (i.e., covariate shift); ii) data imbalance: attack data is often underrepresented, leading to high false negative rates; iii) insufficient real-time performance: many DL-based models are resource-heavy, limiting deployment on edge devices; and iv) limited generalization: solutions tuned to specific datasets often perform poorly in heterogeneous environments. To address these gaps, this paper introduces the dynamic attack pattern-aware (DAPA) improvised weighted gradient boosting (IWGB) framework. It leverages real-time statistical monitoring and adaptive learning to detect covariate shifts, ensuring robust and low-latency detection. This work aims to fill the need for scalable, adaptive, and lightweight IDS for distributed CPS.

Conventional ML and DL-based IDS are insufficient for IoT-edge environments due to their inability to adapt to evolving network behaviors, handle data imbalance, and operate efficiently on constrained devices. There is a need for a dynamic, lightweight, and robust intrusion detection framework that can effectively detect and respond to network-level threats in real time across heterogeneous CPS platforms. This paper proposes the dynamic attack pattern-aware improvised weighted gradient boosting (DAPA-IWGB) model, a novel hybrid intrusion detection approach tailored for IoT-edge-enabled CPS. The model integrates extreme gradient boosting (XGBoost) with an improvised weighted loss function that dynamically adjusts to covariate shifts in network traffic. A statistical monitoring mechanism is embedded to detect real-time distributional changes, allowing the model to adapt continuously. The architecture is designed for edge deployment, minimizing computational load while maintaining high detection accuracy. The model is trained and evaluated on two benchmark datasets UNSW-NB15 [32] and ToN-IoT [33] using stratified sampling and class-balancing strategies to overcome data imbalance. The system demonstrates enhanced adaptability, lower false positive rates, and faster detection times compared to existing IDS models. Proposes an adaptive IDS that detects novel attacks using dynamic weighted learning. Effectively handles covariate shift using real-time statistical monitoring. Enhances detection accuracy on benchmark datasets with minimal false positives. Optimized for deployment on edge devices with low computational overhead. Strengthens IoT-edge CPS resilience against evolving cyber threats.

Section 1 presents the background and a detailed literature review of recent IDS using ML and DL in IoT-edge environments. Then, highlights the research gap and provides the motivation behind developing the DAPA-IWGB model. Further, defines the problem statement and discusses the limitations of existing systems, and research methodology. Section 2, describes the proposed DAPA-IWGB methodology, including model components, architecture, and real-time adaptation strategy. Section 3 provides experimental setup details, datasets used, evaluation metrics, and a comprehensive performance analysis. Section 4 concludes the paper with a summary of key findings and outlines possible future research directions.

2. METHOD

The DAPA-IWGB model, specifically designed for intrusion detection in IoT-edge-enabled CPS, is presented in this part along with a thorough methodology for its design and implementation. The proposed framework is structured to identify and respond to evolving and diverse cyber threats across distributed IoT environments. Initially, we describe the architectural design of the IoT-edge threat detection system, followed by a formal presentation of the underlying mathematical model supporting the DAPA-IWGB hybrid classification approach.

Figure 2 illustrates a representative IoT-edge architecture capturing typical network interactions and potential security vulnerabilities within a heterogeneous CPS. In this paradigm, various IoT devices including smart sensors, wearables, industrial monitors, and home automation systems communicate data to localized edge computing nodes, which perform low-latency preprocessing tasks. Despite the operational benefits of edge computing, the statement pathway among IoT devices and edge nodes remains susceptible to a wide spectrum of security threats. As highlighted in red in the architecture, certain nodes may be compromised and exploited to initiate cyber-attacks, such as: spoofing and impersonation within domain name resolution protocols, denial of service (DoS)/DDoS attacks leading to service disruption, and link-level or routing attacks, corrupting the data flow and device synchronization. These vulnerabilities can degrade system reliability, introduce delays, and compromise sensitive information. To counteract these evolving threat vectors, we propose the DAPA-IWGB intrusion detection model embedded within the edge layer. By leveraging lightweight ensemble learning with dynamic re-weighting mechanisms, the model performs continuous threat monitoring, adapts to concept drift in network behavior, and maintains detection performance over time. Two well-known real-world intrusion detection datasets are used to validate the model: The UNSW-NB15 dataset, which spans nine threat classes and includes a combination of artificial and real network traffic that represents both contemporary and conventional attack categories. Telemetry, operating system logs, and network-based intrusion events gathered from smart devices and edge systems make up the ToN-IoT dataset, which was created for heterogeneous IoT environments. Together, these datasets support comprehensive evaluation of the DAPA-IWGB model across varied attack patterns, data modalities, and real-world CPS deployment scenarios. By deploying the proposed detection mechanism directly at the edge, the system benefits from reduced detection latency, lowered network overhead, and increased responsiveness to localized threats. This architectural design provides a resilient and scalable foundation for securing IoT-edge-enabled CPS against dynamic and multifaceted cyber threats.

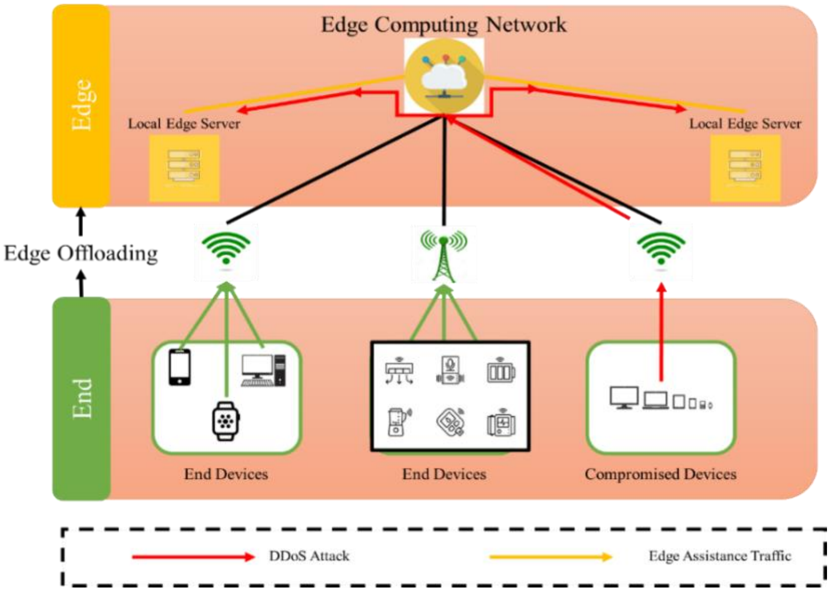

Figure 2. Network communication attack scenario in IoT-edge computing networks

This section introduces the basic working of gradient boosting (XGBoost) model. Further, present an IWGB model for DAPA to optimize the prediction error. The section introduces a new weighted sum prediction error minimization model combined with logarithm-based lost function to design a novel attack predictive classifier; the DAPA-IWGB ensures to reduce the misclassification in the CPS IoT-edge computing networks. Let the input dataset (i.e., UNSW and ToN-IoT) be denoted in (1).

$$X_t = \{(x_1, y_1), (x_2, y_2), \ldots \ldots (x_t, y_t)\} \tag{1}$$

Here, each x_i represents a feature vector at time step t, and $y_i \in \{0,1\}$ denotes the true label, where $y_t = 0$ corresponds to no attack and $y_t = 1$ indicates the presence of an attack. The objective function of the DAPA-IWGB model is formulated as (2). In (2), T is the number of time steps, $\ell(\cdot)$ is the loss function between true label y_t and predicted label y_t, and f_k represents the k^{th} base learner (decision tree). The regularization term $\Omega(f_k)$, which controls model complexity, is defined as (3). Where γ and λ are regularization hyperparameters, and w defines the vector of leaf weights. Each base learner f_k is represented as a weighted sum of leaf predictions, as in (4).

$$L(\theta) = \sum_{t=1}^{T} \ell(y_t, \hat{y}_t) + \sum_{k=1}^{K} \Omega(f_k) \tag{2}$$

$$\Omega(f_k) = \gamma T + \frac{1}{2}\lambda \left|\left|w\right|\right|^2 \tag{3}$$

$$f_k(X_t) = \sum_{j=1}^{T} w_j(t) h_j(X_t) \tag{4}$$

Here, $h_j(X_t)$ is the decision rule for the j^{th} node at time t, and $w_j(t)$ is the corresponding weight. To adapt to varying prediction errors, dynamic weights are computed as in (5). $\bar{\epsilon}_i(t)$ represents the average error for model iii over a recent time window, and $\epsilon_i(t)$ is the instantaneous error. To mitigate volatility in weight updates and ensure temporal stability, an averaged update mechanism is introduced as in (6). Where m denotes the number of prior steps considered for smoothing and $W_i(t-k)$ defines preceding time steps weight of i. The model's prediction error at time t is defined in (7).

$$W_i(t) = \frac{\bar{\epsilon}_i(t)}{\epsilon_i(t)} \tag{5}$$

$$W_i(t) = \frac{1}{m} \cdot \sum_{k=1}^{m} W_i(t-k) \tag{6}$$

$$e_{i,t} = \sum_{i=1}^{N} W_i(t) \cdot f_k(X_t) - f_k(t) \tag{7}$$

$W_i(t)$ defining weighted value assigned at time instance i, $f_k(X_t)$ defines outcome of baseline classifier f_k for X_t, and $f_k(t)$ defines the real value at instance t. Therefore, the error is dynamically recalculated for the next time step as in (8). The final prediction of the ensemble is a weighted sum of tree predictions as shown in (9). The loss function is initially formulated as a binary cross-entropy with class imbalance consideration as shown in (10). However, the loss function with class imbalance parameter α ignoring biased weighting issues considering imbalanced data.

$$e_{i+1,t} = \sum_{i=1}^{N} W_{i+1}(t) \cdot f_{i+1}(X_{i+1}) - f_k(t) \tag{8}$$

$$\hat{y}_t = \sum_{i=1}^{N} f_k(X_t) W_i(t) \tag{9}$$

$$Loss = -\sum_{i=1}^{m} (\alpha y_t \log(\hat{y}_t) + (1 - y_t) \log(1 - \hat{y}_t)) \tag{10}$$

Thus, to further address data imbalance, the class-specific weights α_0 and α_1 are incorporated as in (11). The α_0 weight is kept lower than the α_1 to reduce the false positives. Therefore, the weights are determined based on inverse class frequency as in (12). Where P_{y_t} defines the ration between normal and malicious packet. The updated model weight expression integrating class imbalance becomes (13).

$$Loss = -\sum_{i=1}^{m} (\alpha_1 y_t \log(\hat{y}_t) + \alpha_0 (1 - y_t) \log(1 - \hat{y}_t)) \tag{11}$$

$$\alpha_{yt} = \frac{1}{P_{y_t}}, y_t \in \{0,1\} \tag{12}$$

$$W_i(t) = \frac{\sum_{i=1} (\bar{\epsilon}_i(t) \cdot \alpha_{y_t})}{\epsilon_i(t)} \tag{13}$$

Further, individual tree weights are penalized if misclassifying minority class instances as in (14). Where β defining the penalizing term used for reducing the weight of false positive classifier form minority classes. Therefore, all tree weights are normalized after each period as in (15). Underperforming trees with weights below a predefined threshold θ are pruned as in (16). Where θ is used as a threshold parameter for optimizing the tree size to attain desired attack detection accuracy without overfitting problems.

$$w_j = \beta w_j, \text{ if } H_j(x_t) \neq y_t \text{ and } y_t = 1 \tag{14}$$

$$w_j = \frac{w_j}{\sum_j w_j} \tag{15}$$

$$\mathcal{H} = \frac{\mathcal{H}}{\{H_j | w_j < \theta\}} \tag{16}$$

This section introduces DAPA combined with IWGB for covariate shift handling and model adaptation. The model addresses concept drift and evolving attack patterns using an adaptive ensemble-based training strategy, summarized in Algorithm 1.

Algorithm 1. DAPA-IWGB ensemble adaptation model for intrusion detection in IoT-edge networks

```
Input     Dataset $X_t$, DAPA-IWGB ensemble model index $i$, number of models $N$, attack class $c$, tree
          pruning threshold $\theta$, dynamic penalty factor $\beta$, update interval $p$, and Number of folds $K$
Output    Updated ensemble $H_j$ in DAPA-IWGB and node weights $w_j$
1.        Initialize:
              Set number of trees $m = 1$, initialize all weights $w_j = 1$
              Partition dataset $X_t$ into $K$ folds
2.      For each fold $k = 1$ to $K$ do
              Use fold $k$ as validation set and remaining folds as training data
              Train DAPA-IWGB model on training data
              Initialize ensemble $H = \{H_j\}$
3.      For each time step $t = 1$ to $T$ do
              For each model $i = 1$ to $N$ do
                For each tree $j = 1$ to $m$ do
                  If $H_j(x_t) \neq y_t$ and $(imodp) \neq 0$ then
                    Update tree weight: $w_j = \beta \cdot w_j$
                  End If
                End For
                Compute ensemble prediction using: $f_k(X_t) = \sum_{j=1}^{T} w_j(t) h_j(X_t)$
                If $(imodp) = 0$ then
                  Normalize weights:
                    $w_j = \frac{w_j}{\sum_j w_j}$
                  Prune low-weight trees:
                    $\mathcal{H} = \frac{\mathcal{H}}{\{H_j | w_j < \theta\}}$
                  If predicted $\hat{y}_t \neq y_t$ then
                    Increase number of trees: $m = m + 1$
                    Generate new tree via feature-split:
                      $h_j(x_t)$
                    Add new tree: $\mathcal{H} = H_j \cup h_j(X_t)$, set $w_j = 1$
                  End If
                End If
                For each tree $j = 1$ to $m$ do
                  Update tree $H_j$ with new data:
                    $H_j = (H_j, x_t, y_t)$
                End For
              End For
          End For
4.      Return: Final ensemble $H_j$ and weights $w_j$
```

Algorithm 1 describes the training and adaptation process of the DAPA-IWGB model for intrusion detection in IoT-edge enabled CPS. This model dynamically handles covariate shift, concept drift, and class imbalance while improving classification accuracy across evolving attack patterns. The main components and workflow are explained as:

i) Initialization and K-fold setup: the dataset X_t is partitioned into K non-overlapping folds to enable cross-validation. One-fold is used for validation while the remaining $K - 1$ folds are used for training. This approach improves the generalizability of the model by reducing overfitting and ensures robustness across varied data segments. Each decision tree in the ensemble is initialized with equal weight $w_j = 1$, and the number of trees mmm begins from one.

ii) Ensemble training over time steps: for every time step ttt, the algorithm iterates over each base learner iii in the ensemble of size N. The model uses the DAPA-IWGB framework to build decision trees H_j which are capable of capturing distinct attack patterns.

iii) Error-based weight adjustment: if a decision tree HjH_jHj incorrectly classifies the input sample ($H_j(x_t) \neq y_t$) and the iteration index i is not aligned with the tree update interval p, the weight w_j is penalized using a decay factor β. This mechanism ensures that less accurate trees gradually lose influence over time.

iv) Prediction and ensemble aggregation: the overall prediction at time step t is obtained using a weighted sum of outputs from all decision trees based on (4). The model dynamically adapts its prediction strategy to current input conditions.

v) Periodic tree weight normalization and pruning: at specified intervals (every p iterations), the following actions are triggered: weight normalization: tree weights are scaled relative to the total sum to maintain a consistent influence range. Tree pruning: trees whose weights fall below a predefined threshold θ are considered underperforming and are removed from the ensemble.

vi) Ensemble expansion: if the ensemble misclassifies the current input ($\hat{y}_t \neq y_t$), a new decision tree is added by performing a fresh feature-based split. This ensures that the model learns from recent errors and adapts to evolving attack behavior.

vii) Covariate shift adaptation: to address the problem of covariate shift, each tree H_j is updated at every time step with the latest instance (x_t, y_t). This allows the decision trees to evolve continuously by learning from new and potentially shifted data distributions, ensuring that the model stays relevant in dynamic CPS environments.

viii) Final output: the algorithm outputs the updated ensemble of decision trees H_j and their respective weights w_j, which are optimized through dynamic adjustment, pruning, and cross-validation. This optimized ensemble is then used to predict attacks on future unseen inputs.

Key advantages of the algorithm are: i) dynamic weighting: poorly performing trees lose influence over time, and trees that capture new attack patterns are added adaptively; ii) covariate shift handling: each tree is updated with new samples, maintaining prediction relevance over time; iii) imbalance-aware learning: class-specific weighting (incorporated in loss function and tree weighting) ensures that minority class attacks are not overlooked; iv) K-fold optimization: prevents overfitting by validating performance across multiple data partitions, enhancing generalization; and v) model scalability: ensemble size is adaptively controlled via pruning and addition of trees based on performance. This approach ensures continuous learning from real-time data by dynamically adjusting decision trees, updating leaf weights based on misclassification of rare attack types, and pruning less informative models. The inclusion of class-based weighting, covariate shift handling, and periodic normalization ensures resilience against class imbalance and temporal data drift in IoT-edge-based CPS environments.

3. EXPERIMENTAL SETUP AND RESULTS

The proposed DAPA-IWGB framework was developed and deployed within a simulated IoT-edge computing environment to evaluate its effectiveness in real-time attack detection. Python 3 was used for the implementation, and the detection component was integrated at the edge layer to enable local decision-making and low-latency threat prediction. A computer system with an Intel Core i7 processor and 16 GB of RAM was used for the experiments, guaranteeing enough processing power for both training and inference without sacrificing performance.

Two popular cybersecurity benchmark datasets, UNSW-NB15 and ToN-IoT, which provide thorough coverage of contemporary cyber-attack trends in IoT contexts, were used in the evaluation. UNSW-NB15 [32]: this dataset, which was created by the Australian centre for cyber security (ACCS), includes both benign and malicious network traffic from nine different attack types, such as backdoors, worms, DoS, analysis, exploits, and spamming. It includes 49 network features that capture behavioral characteristics critical for anomaly detection. This dataset provides a robust testbed for evaluating IDS models on conventional and complex network threats. ToN-IoT [33]: building upon the UNSW-NB15 framework, the ToN-IoT dataset incorporates data from real-world IoT infrastructures, encompassing system logs, telemetry, and network activity across multiple layers. Attack types include ransomware, backdoors, link-layer attacks, malware infections, and DoS attacks. This dataset effectively simulates dynamic IoT environments and offers multi-source, heterogeneous data streams, enabling robust training and testing of edge-based intrusion detection models. These datasets were selected for their high relevance to contemporary IoT-edge CPS deployments and their ability to reflect real-world threat scenarios in smart environments.

Standard classification measures were used to evaluate the DAPA-IWGB model's detection performance. These metrics, which measure how well the model distinguishes between attack and normal traffic, are as in (17) to (20).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

$$Precision = \frac{TP}{TP+FP} \tag{18}$$

$$Recall = \frac{TP}{TP+FN} \tag{19}$$

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{20}$$

Where TP, TN, FP, and FN indicate true positive, true negative, false positives, and false negative, respectively. Together, these metrics gives a holistic view of detection accuracy, sensitivity, and robustness to false alarms.

The performance of the DAPA-IWGB model was evaluated across both datasets using the aforementioned metrics. Experimental outcomes on UNSW-NB15 dataset are presented in Figure 3, where the model achieved an accuracy of 99.93%, precision of 99.965%, recall of 99.967%, and F1-score of 99.961%. These results affirm the model's high precision in identifying malicious traffic and its low rate of false positives. The integration of dynamic statistical monitoring and adaptive retraining, as detailed in (12), further strengthens detection stability over time by recalibrating tree weights in response to evolving patterns. Similarly, results on the ToN-IoT dataset are shown in Figure 4, with the following metrics observed an accuracy: 99.921%, precision of 99.92%, recall of 99.85%, and F1-score of 99.85%. The high detection scores across both datasets validate the generalizability and adaptability of DAPA-IWGB under diverse attack conditions. The model's responsiveness to temporal shifts in data distribution is facilitated by a retraining mechanism, which updates ensemble tree structure and weight distribution based on real-time feedback and classification errors. This adaptive learning mechanism ensures long-term reliability in fast-changing IoT environments. Overall, the results demonstrate that DAPA-IWGB effectively distinguishes between normal and malicious behavior, maintains resilience against concept drift, and minimizes classification errors in edge-based CPS infrastructures.

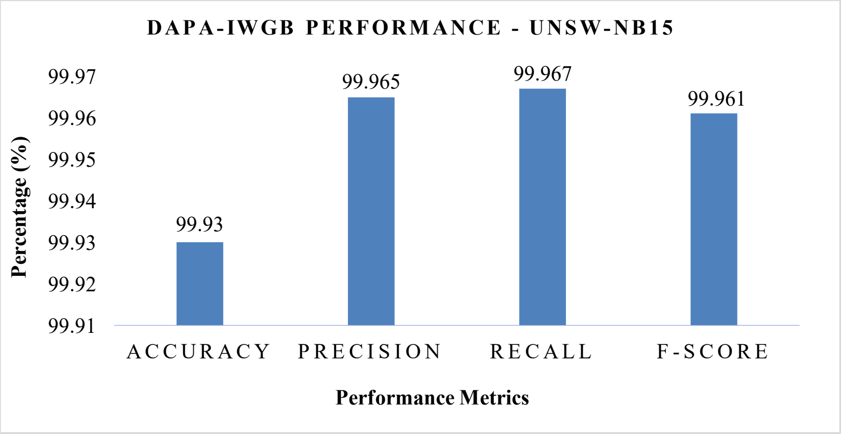

Figure 3. DAPA-IWGB performance on UNSW-NB15 dataset

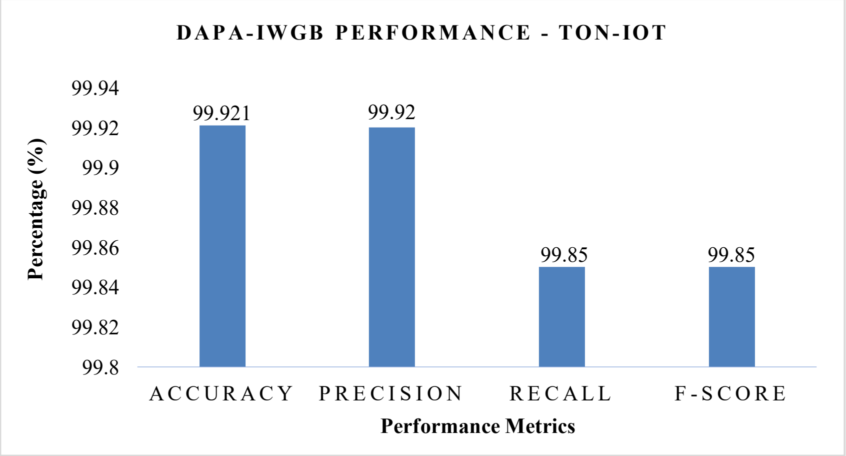

Figure 4. DAPA-IWGB performance on ToN-IoT dataset

The suggested DAPA-IWGB architecture was compared to a number of current and well-known intrusion detection models in IoT-Edge contexts in order to further assess its efficacy and resilience. A review of performance metrics from the literature, including as accuracy, precision, recall, and F1-score, is shown in Table 1. It is clear from Table 1 that the suggested DAPA-IWGB model performs better than current methods in every significant performance category. The model achieved an accuracy of 99.921%, a precision of 99.92%, recall of 99.85%, and an F1-score of 99.85%, demonstrating superior classification capability.

Table 1. DAPA-IWGB performance comparison with existing approaches using the ToN-IoT dataset

Reference/Year	Model	Accuracy	Precision	Recall	F1-score
Logeswari *et al.* [17], 2025	HFOMC	98.83	98.56	98.81	98.65
Saiyed and Al-Anbagi [18], 2024	GATDD	95	95	95	94
Cui *et al.* [19], 2024	DRN-AM	99.24	99.18	99.15	99.16
Javeed *et al.* [20], 2024	IDS-SAEL	99.55	99.31	99.24	99.39
Yang *et al.* [21], 2024	GAD-ELAR	97.67	98.21	97.67	97.84
Bouzinis *et al.* [22], 2025	StatAvg	93.38	-	-	61.22
Fares *et al.* [23], 2025	ST-LSTM-DTL	98.8	98.24	98.67	98.45
Li et al. [24], 2025	SMVL	98.7	-	-	92.5
Chandnani *et al.* [29], 2025	Fed-MLDL	98.1	98.3	98.3	98.3
This research	DAPA-IWGB	99.921	99.92	99.85	99.85

Compared to deep recurrent models such as genetic algorithm employing t-Test-based DDoS detection (GATDD) [18], hybrid models like DRN-AM [19] and IDS-SAEL [20], and the DAPA-IWGB exhibits a notable increase in both precision and recall, indicating a reduced false positive rate and improved sensitivity to actual intrusions. Models such as hybrid feature optimization through multi-stage classifier (HFOMC) [17] and ST-LSTM-DTL [23] perform reasonably well; however, their metrics remain marginally lower than DAPA-IWGB, particularly in F1-score, which indicates a balance between precision and recall. The GATDD [18] model, although based on ensemble principles, records a lower performance (F1-score of 94%), highlighting limitations in dynamic pattern detection in evolving IoT environments. Moreover, the performance of models like StatAvg [22] and SMVL [24] suggests significant trade-offs in detection performance, with either incomplete metric reporting or comparatively lower F1-scores. Notably, Fed-MLDL [29] achieves competitive results, yet still underperforms relative to DAPA-IWGB, particularly in capturing rare and evolving attack instances due to its static federated design.

The superior results of DAPA-IWGB can be attributed to its: dynamic weight adjustment, which reduces model bias toward majority classes, real-time tree pruning and augmentation, enabling adaptability to attack evolution. In addition, statistical monitoring facilitates timely retraining in response to distributional shifts. In summary, the DAPA-IWGB framework demonstrates state-of-the-art performance across standard benchmarks and validates its efficacy for securing IoT-edge-enabled CPS against a wide range of cyber threats.

Using the UNSW-NB15 benchmark dataset, a comparative performance evaluation was carried out to verify the robustness and detection accuracy of the suggested DAPA-IWGB model. The performance of DAPA-IWGB is shown in Table 2 alongside many newly released intrusion detection models that have also used the UNSW-NB15 dataset as an evaluation benchmark. The suggested DAPA-IWGB considerably outperforms all evaluated models across all assessment metrics, as shown in Table 2. With 99.93% accuracy, 99.965% precision, 99.967% recall, and 99.961% F1-score, it significantly outperforms current methods.

Table 2. DAPA-IWGB performance comparison with existing approaches using UNSW-NB15 benchmark

Reference/Year	Model	Accuracy	Precision	Recall	F1-score
Cui *et al.* [19], 2024	DRN-AM	89.23	883.83	87.77	88.25
Yang *et al.* [21], 2024	GAD-ELAR	98.84	98.8	98.84	98.78
Li *et al.* [24], 2025	SMVL	97.9	-	-	85.6
Li et al. [25], 2025	SLRF	90.43	87.69	83.12	-
Wu *et al.* [26], 2025	TRACER	86.02	-	-	-
Bian and Liu [28], 2025	GMCWAE	81.1	-	-	-
Elaziz *et al.* [30], 2025	TTF-EEFO	98.50	98.30	98.20	98.25
This research	DAPA-IWGB	99.93	99.965	99.967	99.961

Compared to recent DL approaches such as GAD-ELAR [21] and framework based on the tab transformer-electric eel foraging optimization (TTF-EEFO) [30], which also exhibit high accuracy and balanced detection performance, the DAPA-IWGB model yields a noticeable improvement in precision and recall, reflecting its enhanced ability to distinguish between benign and malicious traffic with minimal false alarms. The F1-score improvement further demonstrates the proposed model's capability to maintain detection consistency even in the presence of imbalanced data distributions. Other models like. DRN-AM [19], SMVL [24], and SLRF [25], suffer from lower accuracy and recall, indicating sensitivity to feature variability and attack diversity. Additionally, some models such as TRACER [26], ReMeNet [27], and GMCWAE [28] report only partial metrics, making comprehensive comparison difficult but still highlighting their limitations in achieving holistic threat detection.

The performance advantages of DAPA-IWGB can be attributed to its: i) dynamic attack pattern adaptation, which enables learning from evolving threats; ii) covariate shift handling through adaptive ensemble updating; iii) minority class re-weighting and pruning strategies, which prevent bias toward majority classes; and iv) real-time weight optimization and retraining, enhancing robustness across varying traffic patterns. These results affirm that the DAPA-IWGB model is highly suitable for real-time intrusion detection in IoT-edge-enabled CPS environments, offering superior performance compared to existing ML and DL-based intrusion detection techniques on the UNSW-NB15 dataset.

4. CONCLUSION

The rapid creation of the IoT has revolutionized CPS by enabling real-time data exchange between smart devices, edge nodes, and cloud infrastructures. Despite these advancements, securing such heterogeneous and dynamic environments remains a pressing challenge due to the evolving nature of cyber threats and the limitations of conventional detection methods. To address this issue, this paper proposed the DAPA-IWGB model, which integrates a statistical monitoring mechanism to dynamically detect and adapt to shifts in attack behavior. The model employs adaptive re-weighting, real-time tree pruning, and covariate shift handling to maintain high detection fidelity in complex IoT-edge scenarios. Experimental evaluations using two benchmark datasets, UNSW-NB15 and ToN-IoT, demonstrated the effectiveness of the proposed approach. The DAPA-IWGB model achieved superior performance, with accuracy levels of 99.93% and 99.921%, respectively, while maintaining high precision and low false positive rates. These results validate the model’s capability to handle class imbalance and concept drift, ensuring reliable intrusion detection in dynamic edge-based CPS environments. As part of future research, we intend to develop a more generalized ensemble-based intrusion detection framework that incorporates hybrid artificial intelligence techniques, such as deep reinforcement learning, federated learning, and graph-based models. This framework will explicitly address issues of data heterogeneity, covariate shift, and class imbalance, and will be evaluated using more realistic and large-scale datasets drawn from IoT, internet of vehicles (IoV), and CPS domains. Such advancements aim to enhance the scalability, resilience, and adaptability of IDS in next-generation intelligent infrastructures

ACKNOWLEDGMENTS

We would like to thank our supervisor for his assistance, constant feedback, and motivation for the entire duration of the research.

FUNDING INFORMATION

No funding is raised for this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Vishala Ibasapura Lakshminarayanappa	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Kempahanumaiah M. Ravikumar	✓	✓			✓	✓		✓	✓	✓	✓	✓		

C	: **C**onceptualization	I	: **I**nvestigation	Vi	: **Vi**sualization
M	: **M**ethodology	R	: **R**esources	Su	: **Su**pervision
So	: **So**ftware	D	: **D**ata Curation	P	: **P**roject administration
Va	: **Va**lidation	O	: Writing - **O**riginal Draft	Fu	: **Fu**nding acquisition
Fo	: **Fo**rmal analysis	E	: Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest.

DATA AVAILABILITY

The datasets utilized in this research are provided in references [32], [33].

REFERENCES

[1] K. K. Eren, K. Küçük, F. Özyurt, and O. H. Alhazmi, “Simple yet powerful: machine learning-based IoT intrusion system with smart preprocessing and feature generation rivals deep learning,” *IEEE Access*, vol. 13, pp. 41435–41455, 2025, doi: 10.1109/ACCESS.2025.3547642.

[2] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, “Edge computing and cloud computing for internet of things: a review,” *Informatics*, vol. 11, no. 4, 2024, doi: 10.3390/informatics11040071.

[3] G. I. Arcas, T. Cioara, I. Anghel, D. Lazea, and A. Hangan, “Edge offloading in smart grid,” *Smart Cities*, vol. 7, no. 1, pp. 680–711, 2024, doi: 10.3390/smartcities7010028.

[4] S. Ismail, S. Dandan, and A. Qushou, “Intrusion detection in IoT and IIoT: comparing lightweight machine learning techniques using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset datasets,” *IEEE Access*, vol. 13, pp. 73468–73485, 2025, doi: 10.1109/ACCESS.2025.3554083.

[5] S. K. Sahu and K. Mazumdar, “Exploring security threats and solutions techniques for internet of things (IoT): from vulnerabilities to vigilance,” *Frontiers in Artificial Intelligence*, vol. 7, 2024, doi: 10.3389/frai.2024.1397480.

[6] H. Wang, F. Kandah, T. Mendis, and L. Medury, “Clustering-based intrusion detection system meets multi-critics generative adversarial networks,” *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 16112–16128, 2025, doi: 10.1109/jiot.2025.3533918.

[7] N. Singh, R. Buyya, and H. Kim, “Securing cloud-based internet of things: challenges and mitigations,” *Sensors*, vol. 25, no. 1, 2024, doi: 10.3390/s25010079.

[8] R. Uddin, S. A. P. Kumar, and V. Chamola, “Denial of service attacks in edge computing layers: taxonomy, vulnerabilities, threats and solutions,” *Ad Hoc Networks*, vol. 152, 2024, doi: 10.1016/j.adhoc.2023.103322.

[9] P. Mahadevappa, R. Al-amri, G. Alkawsi, A. Alkahtani, M. Alghenaim, and M. Alsamman, “Analyzing threats and attacks in edge data analytics within IoT environments,” *IoT*, vol. 5, no. 1, pp. 123–154, 2024, doi: 10.3390/iot5010007.

[10] S. Yaras and M. Dener, “IoT-based intrusion detection system using new hybrid deep learning algorithm,” *Electronics*, vol. 13, no. 6, 2024, doi: 10.3390/electronics13061053.

[11] I. Priyadarshini, “Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning,” *Big Data and Cognitive Computing*, vol. 8, no. 3, p. 21, 2024, doi: 10.3390/bdcc8030021.

[12] M. F. Saiyed and I. Al-Anbagi, “Deep ensemble learning with pruning for DDoS attack detection in IoT networks,” *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 596–616, 2024, doi: 10.1109/tmlcn.2024.3395419.

[13] M. S. Alshehri, O. Saidani, F. S. Alrayes, S. F. Abbasi, and J. Ahmad, “A self-attention-based deep convolutional neural networks for IIoT networks intrusion detection,” *IEEE Access*, vol. 12, pp. 45762–45772, 2024, doi: 10.1109/ACCESS.2024.3380816.

[14] M. A. Elaziz, I. A. Fares, and A. O. Aseeri, “CKAN: convolutional kolmogorov–arnold networks model for intrusion detection in IoT environment,” *IEEE Access*, vol. 12, pp. 134837–134851, 2024, doi: 10.1109/ACCESS.2024.3462297.

[15] C. J. Chandnani, V. Agarwal, S. C. Kulkarni, A. Aren, D. G. B. Amali, and K. Srinivasan, “A physics-based hyper parameter optimized federated multi-layered deep learning model for intrusion detection in IoT networks,” *IEEE Access*, vol. 13, pp. 21992–22010, 2025, doi: 10.1109/ACCESS.2025.3535952.

[16] A. Berguiga, A. Harchay, and A. Massaoudi, “HIDS-IoMT: a deep learning-based intelligent intrusion detection system for the internet of medical things,” *IEEE Access*, vol. 13, pp. 32863–32882, 2025, doi: 10.1109/ACCESS.2025.3543127.

[17] G. Logeswari, J. D. Roselind, K. Tamilarasi, and V. Nivethitha, “A comprehensive approach to intrusion detection in IoT environments using hybrid feature selection and multi-stage classification techniques,” *IEEE Access*, vol. 13, pp. 24970–24987, 2025, doi: 10.1109/ACCESS.2025.3532895.

[18] M. F. Saiyed and I. Al-Anbagi, “A genetic algorithm- and T-test-based system for DDoS attack detection in IoT networks,” *IEEE Access*, vol. 12, pp. 25623–25641, 2024, doi: 10.1109/ACCESS.2024.3367357.

[19] B. Cui, Y. Chai, Z. Yang, and K. Li, “Intrusion detection in IoT using deep residual networks with attention mechanisms,” *Future Internet*, vol. 16, no. 7, 2024, doi: 10.3390/fi16070255.

[20] D. Javeed, T. Gao, M. S. Saeed, and P. Kumar, “An intrusion detection system for edge-envisioned smart agriculture in extreme environment,” *IEEE Internet of Things Journal*, vol. 11, no. 16, pp. 26866–26876, 2024, doi: 10.1109/jiot.2023.3288544.

[21] C. Yang, L. Wu, J. Xu, Y. Ren, B. Tian, and Z. Wei, “Graph learning framework for data link anomaly detection,” *IEEE Access*, vol. 12, pp. 114820–114828, 2024, doi: 10.1109/ACCESS.2024.3445533.

[22] P. S. Bouzinis *et al.*, “StatAvg: mitigating data heterogeneity in federated learning for intrusion detection systems,” *IEEE Transactions on Network and Service Management*, vol. 22, no. 4, pp. 2944–2955, 2025, doi: 10.1109/tnsm.2025.3564387.

[23] I. A. Fares *et al.*, “Deep transfer learning based on hybrid swin transformers with LSTM for intrusion detection systems in IoT environment,” *IEEE Open Journal of the Communications Society*, vol. 6, pp. 4342–4365, 2025, doi: 10.1109/ojcoms.2025.3569301.

[24] M. Li, Y. Qiao, and B. Lee, “A comparative analysis of single and multi-view deep learning for cybersecurity anomaly detection,” *IEEE Access*, vol. 13, pp. 83996–84012, 2025, doi: 10.1109/ACCESS.2025.3564066.

[25] J. Li, H. Sun, H. Du, L. Li, and Z. Zhang, “Network intrusion detection method based on semi-supervised learning and random forest,” *IEICE Transactions on Communications*, vol. E108-B, no. 10, pp. 1152–1163, 2025, doi: 10.23919/transcom.2024ebp3204.

[26] M. Wu, Y. Zheng, D. S.-H. Wong, Y. Wang, and X. Hu, “TRACER: attack-aware divide-and-conquer transformer for intrusion detection in industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 21, no. 6, pp. 4924–4934, 2025, doi: 10.1109/tii.2025.3547050.

[27] X. Wang, L. Ma, S. K. Das, and Z. Liu, “ReMeNet: a memory-enhanced GAN model for intrusion detection in transportation cyber-physical systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 9, pp. 14264–14276, 2025, doi: 10.1109/tits.2025.3565257.

[28] D. Bian and J. Liu, “GMCWAE: a representation learning technique for network intrusion detection in IoT,” *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 20343–20356, 2025, doi: 10.1109/jiot.2025.3542845.

[29] C. J. Chandnani, V. Agarwal, S. C. Kulkarni, A. Aren, D. G. B. Amali, and K. Srinivasan, “A physics-based hyper parameter optimized federated multi-layered deep learning model for intrusion detection in IoT networks,” *IEEE Access*, vol. 13, pp. 21992–22010, 2025, doi: 10.1109/ACCESS.2025.3535952.

[30] M. A. Elaziz, I. A. Fares, A. Dahou, and M. Shrahili, “Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization,” *Frontiers in Big Data*, vol. 8, 2025, doi: 10.3389/fdata.2025.1526480.

[31] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, “Deep learning-driven methods for network-based intrusion detection systems: a systematic review,” *ICT Express*, vol. 11, no. 1, pp. 181–215, 2025, doi: 10.1016/j.icte.2025.01.005.

[32] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[33] G. Guo, X. Pan, H. Liu, F. Li, L. Pei, and K. Hu, “An IoT intrusion detection system based on TON IoT network dataset,” in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023, pp. 333–338, doi: 10.1109/CCWC57344.2023.10099144.

BIOGRAPHIES OF AUTHORS

Vishala Ibasapura Lakshminarayanappa is presently serving as an assistant professor in the Department of Electronics and Communication, SJC Institute of Technology. With 13.5 years of teaching experience, she has been actively involved in shaping the academic and research landscape in her field. Her area of specialization lies in digital communication and networking, where she has contributed significantly through her teaching and research endeavors. She has a keen interest in communication and signal processing, focusing on advancing knowledge and innovative applications in these domains. She can be contacted at email: vishalail_12@rediffmail.com.

Kempahanumaiah M. Ravikumar is the principal of Bengaluru's VIT at the moment. In 1999, he graduated with a Bachelor of Science in Electronics and Communication Engineering from Bangalore University in Bengaluru. In 2002, he continued his study by earning a master's degree in Biomedical Instrumentation from Sri Jayachamarajendra College of Engineering (SJCE), Mysore, which is connected to VTU, Belgaum. His desire to learn more drove him to seek a Ph.D. in Digital Signal Processing at Nitte Meenakshi Institute of Technology (NMIT), Bangalore, which is connected to VTU, Belgaum. He finished his studies in 2011. He can be contacted at email: kmravikumar75@gmail.com.