Mathematical Modelling of Engineering Problems
Vol. 13, No. 1, February, 2026, pp. 67-77
Journal homepage: http://iieta.org/journals/mmep

Secure and Reliable Intrusion Detection System for Cyberattack Detection in IoT-Edge-Enabled Cyber-Physical Systems

Upasana Mahanjan*, J. Somashekar, Vikram Neerugatti

Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bengaluru 562112, India

Corresponding Author Email: upasanamahajan1@gmail.com

https://doi.org/10.18280/mmep.130107

Received: 6 October 2025
Revised: 20 December 2025
Accepted: 27 December 2025
Available online: 28 February 2026

Keywords:
cyber-physical systems, Distributed Denial-of-Service, attack detection, Gradient Tree Multi-Layer Perceptron, edge computing, Internet-of-Things security, intrusion detection system

ABSTRACT

The rapid growth of Internet of Thing (IoT) environments integrated with edge–cloud infrastructures has intensified security vulnerabilities in cyber-physical systems, particularly against evolving network-level cyberattacks. Although existing machine learning and deep learning–based intrusion detection systems offer promising results, their effectiveness significantly declines when faced with dynamic and sophisticated attack patterns. To address this challenge, this paper proposes a Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security (GTMLP-SRS) framework for adaptive intrusion detection in IoT-edge-enabled cyber-physical systems. The proposed model integrates gradient tree boosting with a multilayer perceptron and incorporates real-time statistical monitoring to support adaptive learning and enhance resilience against emerging threats. Experimental evaluations conducted on the Telemetry over Network (ToN)–IoT and University of New South Wales – Network Behavior 2015 Dataset (UNSW-NB15) benchmark datasets achieve detection accuracies of 99.931% and 99.97%, respectively, outperforming existing intrusion detection methods. Comparative analysis confirms that GTMLP-SRS achieves superior adaptability, accuracy, and reliability, underscoring its effectiveness in strengthening the security of modern IoT-based cyber-physical environments.

1. INTRODUCTION

The fast development of the Internet of Things (IoTs) has significantly reformed the landscape of modern cyber-physical systems, enabling seamless connectivity among smart devices, sensors, edge nodes, and cloud infrastructure [1]. IoT-enabled devices, ranging from consumer wearables to industrial sensors and autonomous vehicles, continuously generate and transmit large volumes of continuous-stream information for intelligent processing and actionable insights [2]. To manage this data efficiently and minimize latency, edge computing has emerged as a fundamental standard by enabling localized data analysis closer to the source [3]. When local computational capacity is exceeded, edge devices seamlessly offload tasks to cloud platforms, facilitating large-scale processing and long-term data storage [4]. This hierarchical data flow across IoT, edge, and cloud layers ensures system-wide responsiveness and scalability in areas like healthcare, smart city, and industrial applications.

Despite the operational benefits of this integrated architecture [5], IoT systems remain highly vulnerable to cyber threats, particularly at the communication layers bridging IoT-Edge and Edge-Cloud nodes [6]. IoT devices possess limited storage, computing power, battery capacity, and processing capabilities; consequently, they present an attractive attack surface for adversaries [7]. Figure 1 illustrates various cyber threats, including domain-based spoofing, Distributed Denial-of-Service (DDoS), and multi-layer link attacks [8].

Cyberattacks such as Man-in-the-Middle (MitM) intrusions, Domain Name System (DNS) spoofing, and DDoS attacks [8], as shown in Figure 1, exploit these vulnerabilities to disrupt services, compromise data integrity, and endanger user privacy [9]. Among these, network-level attacks such as link-flooding DDoS pose a substantial risk by overwhelming edge nodes with malicious traffic, leading to degraded performance and system outages [10].

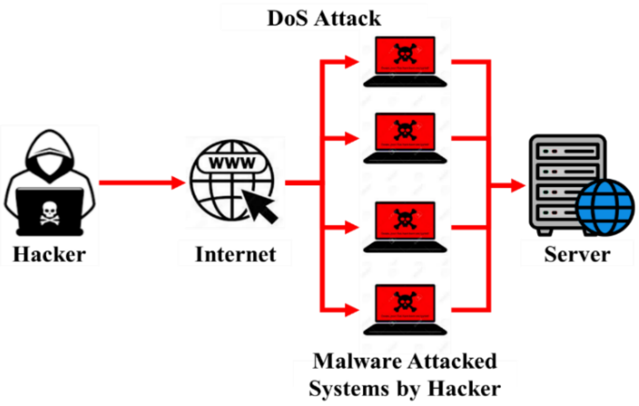


Figure 1. Denial-of-Service (DoS) attack

In recent years, numerous intrusion detection systems (IDSs) [11] based on machine learning and deep learning models have been developed to enhance IoT network security [12, 13]. Machine learning (ML)-based approaches typically rely on handcrafted traffic features, whereas deep learning (DL)-based techniques employ hierarchical neural architectures to capture complex attack patterns. However, existing ML/DL-based IDS suffer from several critical limitations, including high computational overhead unsuitable for resource-constrained IoT-edge environments, poor adaptability to evolving and zero-day attacks, sensitivity to class imbalance in real-world traffic datasets, and delayed threat detection caused by static learning mechanisms [14, 15]. These challenges result in increased misclassification rates and reduced reliability, particularly at the dynamic IoT-Edge-Cloud interface, thereby limiting their effectiveness in real-time cyber-physical systems [16, 17].

From the above discussion, it is evident that current ML and DL-based intrusion detection frameworks lack adaptive learning capability, computational efficiency, and real-time responsiveness, especially under dynamic and large-scale IoT-edge deployments. Existing approaches are often unable to efficiently balance detection accuracy with low latency and scalability, highlighting the need for a lightweight yet adaptive intrusion detection framework capable of addressing evolving attack behaviors at the network and communication layers.

In addressing these shortcomings, this work proposes a new intrusion detection framework, namely Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security (GTMLP-SRS), designed to enhance cybersecurity in IoT-edge-enabled cyber-physical systems. The GTMLP-SRS model integrates gradient-boosted decision trees with a multi-layer perceptron to effectively capture both linear and non-linear patterns in network traffic behavior. By incorporating statistical monitoring and adaptive learning mechanisms, the framework dynamically responds to evolving attack strategies, ensuring timely and accurate threat detection with minimal computational overhead.

The primary research objectives of this work are summarized as follows:

- To design an adaptive intrusion detection framework capable of accurately identifying network- and communication-layer attacks in IoT-edge-enabled cyber-physical systems.
- To integrate gradient tree boosting with a multi-layer perceptron for enhanced feature representation and classification of complex attack patterns.
- To incorporate real-time statistical monitoring to improve adaptability against evolving and previously unseen cyber threats.
- To achieve low-latency and computationally efficient intrusion detection suitable for resource-constrained IoT-edge environments.
- To validate the effectiveness of the proposed GTMLP-SRS framework through benchmark evaluations and comparative analysis with existing ML and DL-based IDS methods.

A scalable and computationally efficient intrusion detection framework is thus proposed, enhancing secure and reliable communication between IoT, edge, and cloud layers. By integrating GTMLP-SRS into the IoT-edge-based architecture, the proposed solution strengthens the overall system security, ensuring resilient and uninterrupted communication across cyber-physical environments.

Section 2 reviews relevant literature on ML and DL-based intrusion detection methods. Section 3 presents the GTMLP-SRS model architecture deployed at the IoT-edge layer. Section 4 discusses experimental results and comparative evaluations. Section 5 concludes the paper with key findings and future research directions.

2. LITERATURE SURVEY

The rapid growth of IoTs devices has brought immense benefits but has also presented noteworthy safety weaknesses. Recent research in intrusion detection in Cyber-Physical Systems (CPSs) has focused on leveraging artificial intelligence to address these challenges effectively. This survey examines recent state-of-the-art contributions in IDS for IoTs networks, concentrating on methodologies, datasets, research significance, and limitations. Logeswari et al. [2] presented Capsule Networks, Attention Augmented–Recurrent Neural Network, Quantum-based Particle Swarm Optimization, and Adaptive Neuro–Fuzzy system (CAARQA). The CAARQA combined correlation and entropy-based methods to build hybrid feature selection mechanisms; then, the optimized features are trained using multi-stage classifiers such as gradient-boosting and random-forest. The method is trained using Telemetry over Network (ToN)–IoT and Canadian Institute for Cybersecurity – Internet of Things 2023 (CIC-IoT2023) Dataset and achieved 98.83% accuracy due to effective feature dimensionality reduction and ensemble-based classification. However, high computational complexity in multi-stage classification may limit real-time deployment in edge environments. Saiyed and Al-Anbagi [18] introduced Genetic Algorithm–Driven Anomaly Detector with Ensemble Tree (GADAD-ET) for effective DDoS attack detection (DAD). The GADAD-ET applied evolutionary algorithm like genetic algorithm for selecting the features and a t-test for statistical significance testing, followed by an ensemble tree (ET) classifier. The algorithms are trained by means of the Canadian Institute for Cybersecurity – Intrusion Detection System 2017 (CIC-IDS2017) Dataset and ToN-IoT datasets. The model is effective in detecting DDoS attacks with fewer features. However, is not generalized for multi-class intrusion scenarios beyond DDoS.

Cui et al. [19] introduced the Long Short-Term Memory (LSTM)–ResNet hybrid model by integrating ResNeT with an attention mechanism to capture hierarchical features using realistic network communication profiles. The methodology is validated on ToN-IoT and University of New South Wales – Network Behavior 2015 Dataset (UNSW-NB15) datasets ensuring improved spatial representation and high detection accuracy for complex attacks. However, the model overfitting risks due to depth and requires Graphics Processing Unit (GPU) acceleration. Javeed et al. [20] introduced a lightweight IDS designed using Bidirectional Gated Recurrent Unit–LSTM (Bi-GRU-LSTM) tailored for smart agriculture, considering edge-device limitations and environmental challenges. The model is tested on a custom dataset simulating extreme weather and rural connectivity conditions. Then, the ToN-IoT dataset is employed for generating attacks on IoT devices; the model addresses real-world constraints of agricultural IoT environments. However, limited generalizability beyond the agriculture domain. Yang et al. [21] presented a Graph Neural Network for Anomaly Detection (GNNAD) to model inter-node data link relationships. The model is tested on the UNSW-NB15 and Ton-IoT datasets. The methodology is efficient in capturing topological anomalies often ignored by traditional IDS. However, high training time and complex hyperparameter tuning impact its performance.

Bouzinis et al. [22] modeled StatAvg to mitigate data heterogeneity in federated IDS training. The model performance is studied on two well-known datasets namely ToN-IoT and CIC-IoT2023, enhancing federated learning performance across distributed IoT nodes. However, StatAvg assumes data distribution awareness, which may not be realistic. Fares et al. [23] introduced Swin Transformer–Long Short-Term Memory (ST-LSTM) (with transfer learning). The hybrid architecture ST-LSTM model is trained using ToN-IoT, CIC-2023, Network Security Laboratory – Knowledge Discovery in Databases Dataset (NSL-KDD), Message Queuing Telemetry Transport–Internet of Things (MQTT-IoT) Dataset. The model works well considering heterogeneous IoT datasets; however, it requires significant memory resources and long training periods. Li et al. [24] introduced both single-view Convolutional Neural Network (CNN) and multi-view CNN. The model also considered comparing both single and multi-view by combining different data perspectives of the DL models like Multi-View Auto-Encoder CNN (MV-AE-CNN). The MV-AE-CNN performance is validated on ToN-IoT and UNSW-NB15 datasets. The result demonstrated that multi-view learning outperforms single-view in complex intrusion detection; however, the data synchronization for multi-view processing is challenging in real-time systems.

Li et al. [25] introduced the IDS model namely Semi-Supervised Learner–Random Forest (SSL-RF) to effectively detect attacks using UNSW-NB15 and NSL-KDD datasets. The SSL-RF methodology reduces dependency on labeled data, enhancing scalability. However, the performance depends heavily on the quality of pseudo-labels generated using Semi-Supervised Learning (SSL). Wu et al. [26] introduced an intrusion detection system namely Tactical Reconnaissance Armoured Combat Equipment Requirement (TRACER). The model designed a divide-and-conquer transformer architecture with attack awareness to ensure higher detection accuracy. The model is tested on UNSW-NB15, Edge-Industrial Internet of Things (IIoT), and CIC-IDS2017 datasets. The model achieved a robust accuracy of 86.02% while optimizing resource usage for IoT scenarios. However, attain Sub-optimal performance in detecting rare or zero-day attacks. Wang et al. [27] introduced Residual Memory Network (ReMeNet), by developing a memory-enhanced Generative Adversarial Network (GAN) for anomaly detection in cyber-physical systems. The methodology attains an accuracy of 91.7% on the UNSW-NB15 benchmark. Thereby, ensuring improved detection of temporal patterns via memory augmentation. However, adversarial training instability and mode failure in GANs impact on its overall performance. Bian and Liu [28] presented Generative Memory-Conditioned Wasserstein Autoencoder (GMCWAE) to effectively detect complex attacks. The GMCWAE is trained using CIC-IoT2023, UNSW-NB15, and NSL-KDD, benchmarks. The model ensures high representational fidelity and generalization to multiple IoT datasets. However, reconstruction-based anomaly detection may underperform for sophisticated attack patterns. The detailed survey current IDS methods and its limitation are discussed in Table 1.

Table 1. Summary of related intrusion detection studies in IoT and edge environments

Reference	Datasets	Methodology	Strengths	Limitations
Logeswari et al. [2]	University of New South Wales – Network Behavior 2015 dataset	Hybrid feature selection + multi-stage classification	Improved detection accuracy through feature optimization	High computational cost; limited adaptability to evolving attacks
Saiyedand Al-Anbagi [13]	Canadian Institute for Cybersecurity – Distributed Denial of Service dataset	Genetic algorithm + statistical t-test	Effective Distributed Denial-of-Service detection; reduced false positives	Static learning; limited scalability in edge environments
Cui et al. [19]	Network Security Laboratory – Knowledge Discovery in Databases dataset	Deep residual network with attention	Captures complex spatial features	Requires large training data; high training overhead
Javeed et al. [20]	Telemetry over Network–Internet of Things dataset and Custom agriculture dataset	ML-based intrusion detection system for edge-enabled smart farming	Low-latency detection in extreme environments	Dataset-specific; limited generalization
Yang et al. [21]	Real network traffic	Graph learning-based anomaly detection	Effective link-level anomaly modeling	High memory and processing overhead
Bouzinis et al. [22]	Federated Intrusion Detection System datasets	Federated learning with statistical averaging	Mitigates data heterogeneity	Communication overhead; delayed convergence
Fares et al. [23]	Internet of Things–Intrusion Detection datasets	Swin Transformer + Long Short-Term Memory	High accuracy using deep temporal features	Computationally intensive for IoT-edge nodes
Wu et al. [26]	Industrial Internet of Things datasets	Transformer-based divide-and-conquer intrusion detection system	Robust attack awareness	Model complexity limits real-time deployment
Wang et al. [27]	Cyber-Physical System (CPS) traffic data	GAN with memory enhancement	Effective zero-day detection	Training instability; high resource usage

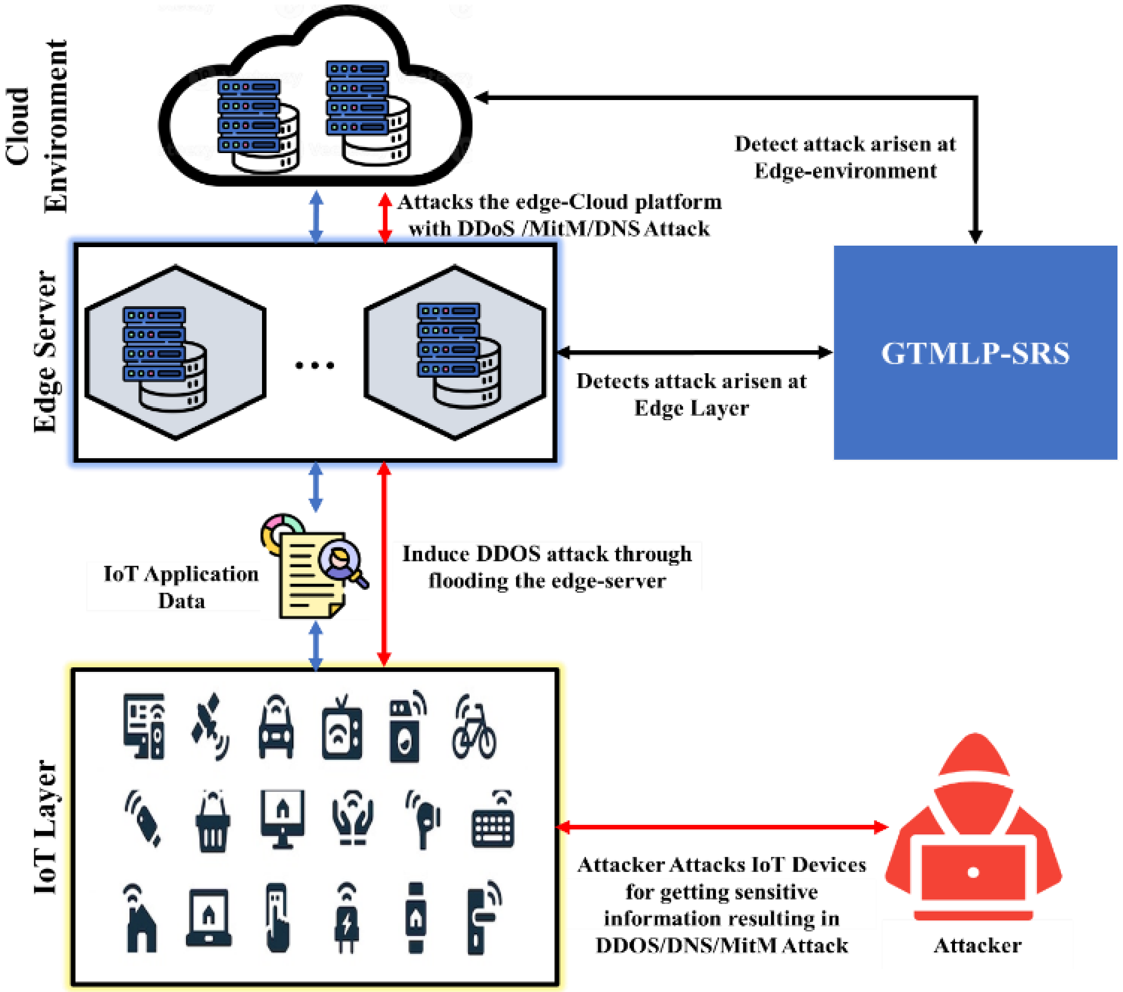
Across the reviewed works in Table 1, there is a notable trend towards ML and DL-based hybrid architectures, transformer-based models, and federated learning approaches to intrusion detection in CPS-IoT networks [29-31]. Most studies rely on popular benchmarks such as CIC-IoT2023, ToN-IoT, and UNSW-NB15, enabling reproducibility and standardized performance evaluation [30, 31]. However, limitations such as high computational overhead, dataset heterogeneity, lack of explainability, and insufficient generalizability across heterogeneous IoT-edge environments persist [29-34]. Recent studies further highlight that edge-intelligent security frameworks, although promising, often struggle with scalability and real-time adaptability in cyber-physical systems [32, 34]. Thus, it is important to design intrusion detection models that emphasize lightweight, adaptive, and explainable architectures, particularly validated on realistic IoT-edge platforms [35]. In meeting this research objective, this paper introduces a novel intrusion detection system for IoT–edge heterogeneous CPS networks, namely GTMLP-SRS, which is presented in the next section.

3. PROPOSED METHODOLOGY

This section presents a methodology for designing GTMLP-SRS. The architecture of detecting securely and reliably attacks in IoT-Edge-based CPS is presented; then, the mathematical model of the proposed GTMLP hybrid classifier is introduced. Then, the secure and reliable security model is presented for the IoT-Edge-based platform.

3.1 IoT-edge threat detection architecture

Figure 2 depicts a representative network and communication path threat scenario within an IoT-Edge-Cloud environment. It captures the interconnectivity between diverse IoT devices such as smart home systems, connected vehicles, and wearable technologies and the underlying edge computing infrastructure. These devices transmit data to nearby edge nodes, which in turn forward the data to cloud platforms for in-depth analysis. However, as illustrated, certain IoT nodes (highlighted in red) are vulnerable to cyber threats, which include spoofing-based domain attacks, DDoS, and multi-layer link attacks. Exploiting these vulnerabilities, adversaries may initiate communication-level attacks capable of disrupting data transmission and compromising device integrity. To mitigate such threats, this study proposes a robust threat detection and prediction framework embedded within the edge layer, referred to as the GTMLP-SRS model.



Cloud Environment
Detect attack arisen at Edge-environment
Attacks the edge-Cloud platform with DDoS /MitM/DNS Attack
Edge Server
GTMLP-SRS
Detects attack arisen at Edge Layer
IoT Application Data
Induce DDOS attack through flooding the edge-server
IoT Layer
Attacker Attacks IoT Devices for getting sensitive information resulting in DDOS/DNS/MitM Attack
Attacker

Figure 2. Network and communication attack scenario in Internet of Thing (IoT) devices in edge enabled network
Note: GTMLP-SRS: Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security; DDoS: Distributed Denial-of-Service; MitM: Man-in-the-Middle; DNS: Domain Name System.

3.2 Gradient tree multi-layer perception-based secure model

Let the time-dependent behavior of IoT-collected observations be denoted by a dataset X, defined as Eq. (1) and here, x_t represents the feature vector at time step t, and $y_t \in \{0,1\}$, where $y_t = 1$ indicates a detected attack and $y_t = 0$ denotes normal behavior. The GTMLP-SRS model F performs a mapping from input features X to output labels y, defined as Eq. (2).

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

$$F = f(X) = \sum_{k=1}^{K} \theta_k \cdot h_k(X) \tag{2}$$

In this expression, K is the number of decision trees within the ensemble, θ_k is the assigned weight to the k^{th} tree, and $h_k(X)$ is the output of that tree for input X. The model's training objective is to minimize a composite loss function composed of binary cross-entropy loss and a regularization term to avoid overfitting in Eq. (3). The first term measures the prediction error between the actual and predicted classes, while the second term introduces a regularization penalty to prevent overfitting. Minimizing this loss function enables the model to learn optimal parameters for accurate intrusion detection. The attack probability p_t is estimated (between 0 and 1) using a sigmoid activation function in Eq. (4). This probabilistic output indicates the likelihood that a given network traffic instance belongs to the attack class, making it suitable for binary intrusion detection tasks. The regularization function $\Omega(h_k)$ for the k^{th} tree is expressed as in Eq. (5).

$$L = \sum_{t=1}^{N} [y_t \log(p_t) + (1 - y_t) \log(1 - p_t)] + \sum_{k=1}^{K} \Omega(h_k) \tag{3}$$

$$p_t = \sigma(f(x_t)) = \frac{1}{1 + e^{-f(x_t)}} \tag{4}$$

$$\Omega(h_k) = \gamma N + \frac{1}{2}\lambda \|w_k\|^2 \tag{5}$$

Here, N denotes the overall leaf node considered within a tree, w_k is the weight vector for leaf nodes, and γ, λ are hyperparameters control model complexity to regulate the magnitude of the Multi-Layer Perceptron (MLP) weights w_k. This regularization mechanism helps reduce model overfitting and enhances generalization by penalizing overly complex models. The GTMLP-SRS model learns optimal splits and weight assignments to balance prediction accuracy and generalizability. To further improve the detection accuracy and competence in attaining generalizability of the GTMLP-SRS model, an MLP is employed to optimize the hyperparameters and facilitate ensemble model construction. The MLP, acting as a meta-learner, is designed to fine-tune key constraints like estimators K, learning rate, tree size, and regularization coefficients γ and λ defined in Eq. (6). The MLP architecture comprises an input-layer consistent to the feature dimensionality with respect to X, then, it has multiple hidden-layers composed of ReLU activations, and an output layer with sigmoid activation to map the final prediction probability. The loss function is designed using binary cross-entropy function for performing the training process of MLP networks through backpropagation algorithm and an adaptive learning rate optimizer. To identify the optimal configuration of the GTMLP-SRS model, a grid-based cross-validation (GridSearchCV) approach is employed. This technique systematically explores combinations of hyperparameters across a predefined search space:

$$H = \{max\ \_depth, learning_{rate}, K, \gamma, \lambda\} \tag{6}$$

In Eq. (6), each candidate set of hyperparameters in H is evaluated which includes key parameters such as *max_depth* and *learning_rate* for the gradient tree component, the number of neurons K in the MLP, and the regularization parameters $\gamma$and λ using k-fold cross-validation (CV) mechanism. A k-fold cross-validation strategy systematically evaluates all possible combinations of these parameters to identify the configuration that provides optimal detection performance. In performing CV, the data considered during training is equally divided into k segments. The GTMLP-SRS is iteratively trained on $k - 1$ folds; the feature weights are optimized and validated with remaining data. The GTMLP-SRS model training performance is studied considering various receiver operating characteristic metrics and are recorded for each configuration. Upon completion, the combination yielding the highest cross-validated performance is selected, and the corresponding GTMLP-SRS ensemble classifier is reconstructed using the optimal parameters. This MLP-driven grid search mechanism ensures that the final model is both well-calibrated and robust against overfitting while maintaining high sensitivity to temporal and statistical shifts in attack behavior.

The MLP employed in the proposed system is a fully connected feedforward neural network that approximates nonlinear mappings between the input IoT behavioral feature space and the binary output space $\{0,1\}$, indicating normal or attack behavior. Let the input feature vector at time t be $x_t \in R^d$, where d is the feature dimension. The MLP consists of L layers, including $L - 1$ hidden-layers and one output-layer. The transformation of the input through the network is defined recursively as follows in Eqs. (7)-(9):

$$z^{(l)} = W^{(l)} a^{(l-1)} + b^{(l)},\ l = 1,2, \dots, L \tag{7}$$

$$a^{(l)} = \phi^{(l)}(z^{(l)}),\ \text{for } l = 1,2, \dots, L \tag{8}$$

$$\hat{y}_t = \sigma(z^{(l)}) = \frac{1}{1+e^{-z^{(L)}}},\ \text{for } l = 1,2, \dots, L \tag{9}$$

Eq. (9) represents the final output layer, where the sigmoid function converts the network output into a probability value between 0 and 1. This probability $\hat{y}_t$ indicates whether a given network traffic instance is classified as normal or malicious, enabling binary intrusion detection in the GTMLP-SRS framework. In these equations: $a^{(l)} = x_t$ is the input layer, $W^{(l)} \in R^{n_l \times n_{l-1}}$ and $b^{(l)} \in R^{n_l}$ are the weighted matrices and bias term at the layer l, $\phi^{(l)}(\cdot)$ is the activation process considering layer l; typically ReLU are used in hidden layers: $\phi(z) = \max(0, z)$, $\sigma(\cdot)$ denotes the sigmoid function used at the output layer for binary classification. The MLP is trained using a dataset $\{(x_t, y_t)\}_{t=1}^{N}$, and the optimization aim are to reduce the loss by employing binary cross-entropy process using below minimization Eq. (10):

$$\mathcal{L}_{MLP} = -\frac{1}{N}\sum_{t=1}^{N} [y_t \log(\hat{y}_t) + (1 - y_t) \log(\hat{y}_t)] \tag{10}$$

Eq. (10) defines the binary cross-entropy loss function used to train the MLP. In this formulation, y_t represents the true label of the t^{th} training sample, while $\hat{y}_t$ denotes the predicted probability output by the MLP. The loss function measures the discrepancy between the predicted and actual labels across all N samples in the dataset. By minimizing this loss during training, the MLP learns model parameters that improve classification accuracy for distinguishing between normal and malicious network traffic in the proposed GTMLP-SRS framework. During training, gradient descent or a variant such as Adam is used to update the weights $W^{(l)}$ and biases $b^{(l)}$ to minimize $\mathcal{L}_{MLP}$. Once trained, the MLP model is used to score and select optimal hyperparameter configurations in the search space H using performance metrics computed using GridSearchCV, where each hyperparameter tuple is evaluated through cross-validation. By integrating MLP in this optimization loop, the GTMLP-SRS model benefits from automatic, data-driven tuning of its structure and training dynamics, improving both attack prediction accuracy and generalization performance across varying IoT environments.

3.3 Secure and reliable security model for Gradient Tree Multi-Layer Perceptron

Given the evolving nature of attack patterns, the model incorporates a statistical adaptation mechanism to detect behavioral drift in real-time. A high divergence value indicates a significant deviation, prompting an update of the time window W. The window is divided into two segments: a stable historical segment S with sub-window S_{sub}, and a recent testing segment T, where $\mid S \mid \gg \mid T \mid$. To statistically validate behavioral changes [36], a two-sample t-test is conducted in Eq. (11):

$$test - t = \frac{\bar{S} - \bar{T} - (\mu_1 - \mu_2 - \delta)}{\sigma_w \sqrt{(\frac{1}{n_1} + \frac{1}{n_2})}} \sim t(n_1 + n_2 - 2) \qquad (11)$$

Eq. (11) represents a two-sample t-test used to statistically verify whether there is a significant behavioral change between historical and recent network traffic patterns. In this formulation, $\bar{S}$, $\bar{T}$ denote the mean values of the stable historical segment and the recent testing segment, respectively. The parameters $n_1$and n_2 represent the sample sizes of these two segments, σ_w indicates the pooled standard deviation, μ_1, μ_2 are population means. The term δ accounts for an allowable threshold between the two segments. The computed test statistic follows a t-distribution with $(n_1 + n_2 - 2)$ degrees of freedom. A high-test statistic value indicates a statistically significant deviation in recent behavior, thereby triggering an update of the time window W for adaptive intrusion detection. If the test indicates significant behavioral change, the window is reset ($W = \emptyset$) and the model is retrained from the updated observation $x_1 = x_2$. Otherwise, the model remains unchanged. Once trained, the GTMLP-SRS model predicts threats in new IoT input streams X_{new} as in Eq. (12).

$$F = f(X_{new}) = \sum_{k=1}^{K} \theta_k \cdot h_k(X_{new}) \qquad (12)$$

Eq. (12) describes the final decision function of the trained GTMLP-SRS model, where the output F is computed as a weighted combination of K learned components $h_k(X_{\text{new}})$. Each component captures distinct behavioral patterns from the incoming IoT data stream X_{new}, and the corresponding weights θ_k reflect their relative importance in the final prediction. The probability of attack occurrence is estimated as in Eq. (13). An attack is flagged ($y = 1$) if p_{attack} surpasses a predefined threshold; otherwise, normal behavior is presumed.

$$p_{attack} = \sigma\big(f(X_{new})\big) \qquad (13)$$

Eq. (13) applies the sigmoid activation function to the aggregated output $f(X_{\text{new}})$, converting it into a probability value p_{attack} between 0 and 1. This probability represents the likelihood of an attack occurrence. If p_{attack} exceeds a predefined threshold, the input is classified as malicious ($y = 1$); otherwise, it is considered normal behavior. This probabilistic decision mechanism enables reliable and adaptive intrusion detection in real-time IoT-edge environments.

3.4 Flow diagram and algorithm

The GTMLP-SRS algorithm operates in six systematic stages to detect network and communication attacks in IoT-edge environments as shown in Algorithm 1. The complete flow of proposed work is given in Figure 2.

Algorithm 1. Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security (GTMLP-SRS)-based secure and reliable attack detection framework

```
Input: Streaming IoT system behavior data
$X = \{(x_1, y_1), (x_2, y_2), \dots (x_t, y_t)\}$. Initial time window $W = \emptyset$, learning rate $\eta$, number of estimators $K$, regularization parameters $\gamma, \lambda$, threshold $\tau$
Output: Attack label $y \in \{0,1\}$ for each incoming observation
Step 1. Initialization:
    Initialize GTMLP-SRS model with parameters $\gamma, \lambda, K$
    Define historical stable window $S \subset X$, current testing window $T$
Step 2. Training phase:
    For each $(x_t, y_t) \in S$:
        Train the GTMLP-SRS model by minimizing the regularized log-loss function:
        $L = \sum_{t=1}^{N} [y_t \log(p_t) + (1 - y_t)\log(1 - p_t)] + \sum_{k=1}^{K} \Omega(h_k)$
        where, $p_t = \sigma\big(f(x_t)\big), \Omega(h_k) = \gamma N + \frac{1}{2}\lambda \big|\big|w_k\big|\big|^2$.
Step 3. Hyperparameter optimization using Multi-Layer Perceptron (MLP) and GridSearchCV:
    Construct an MLP with input $x_t$, hidden layers $L$, and sigmoid output
    Optimize GTMLP-SRS hyperparameters $\{K, \gamma, \lambda, depth\}$ using GridSearchCV with MLP-scored validation
    Select the configuration with the highest cross-validation performance
Step 4. Attack pattern variance detection:
    For each new sample $x_t$, compute KL divergence:
        $D_{KL}(x_t || x_1) = \sum_{x \in X} x_t(x) \log \frac{x_t(x)}{x_1(x)}$
    If $D_{KL}$ exceeds a threshold:
        Append $x_t$ to window $W \leftarrow W \cup x_t$
Step 5. Change point detection with statistical test:
    Partition $W$ into $S_{sub}$ and $T$ such that $\mid S \mid \gg \mid T \mid$
    Perform two-sample t-test:
        $t = \frac{\bar{S} - \bar{T} - (\mu_1 - \mu_2 - \delta)}{\sigma_w \sqrt{(\frac{1}{n_1} + \frac{1}{n_2})}}$
    If a significant change is detected:
        Reset window $W \leftarrow \emptyset$, update reference $x_1 \leftarrow x_t$
        Retrain GTMLP-SRS model using new data
Step 6. Inference phase:
    For each new observation $x_{new}$: $p_{attack} = \sigma\big(f(X_{new})\big)$
    If $p_{attack} > \tau$, classify as attack: $y = 1$; else normal: $y = 0$
Step 7. End of algorithm
```

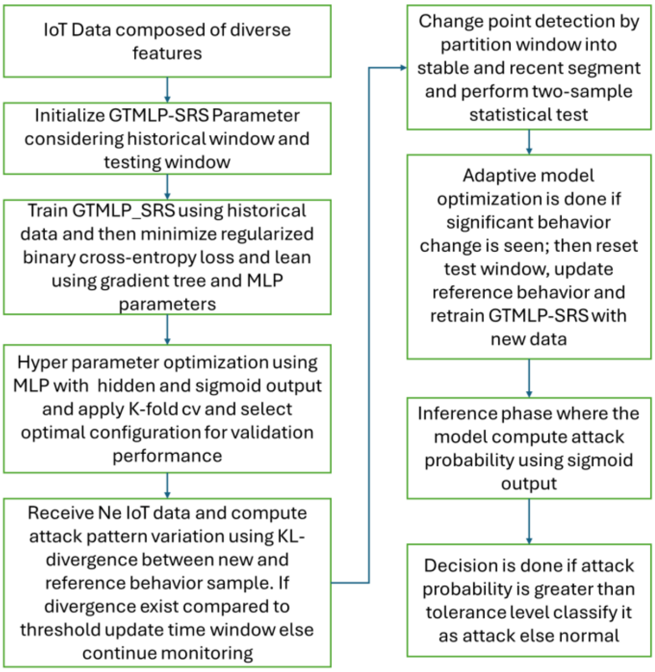

IoT Data composed of diverse features
Initialize GTMLP-SRS Parameter considering historical window and testing window
Train GTMLP_SRS using historical data and then minimize regularized binary cross-entropy loss and lean using gradient tree and MLP parameters
Hyper parameter optimization using MLP with hidden and sigmoid output and apply K-fold cv and select optimal configuration for validation performance
Receive Ne IoT data and compute attack pattern variation using KL-divergence between new and reference behavior sample. If divergence exist compared to threshold update time window else continue monitoring
Change point detection by partition window into stable and recent segment and perform two-sample statistical test
Adaptive model optimization is done if significant behavior change is seen; then reset test window, update reference behavior and retrain GTMLP-SRS with new data
Inference phase where the model compute attack probability using sigmoid output
Decision is done if attack probability is greater than tolerance level classify it as attack else normal

Figure 3. Flow diagram of proposed pipeline model

As shown in Algorithm 1 and Figure 3, initially, the model is trained on historical IoT data using a regularized log-loss function to prevent overfitting. Hyperparameters such as the number of estimators and tree complexity are optimized using a Multi-Layer Perceptron (MLP) with GridSearchCV for enhanced accuracy. As new data arrives, Kullback-Leibler divergence is computed to identify distributional changes in device behavior. If significant divergence is observed, a statistical t-test compares historical and new data to confirm behavioral shifts. Upon detecting a change, the model is retrained with the updated data window. For each new observation, the GTMLP-SRS computes the probability of an attack using a sigmoid-activated output. If this probability exceeds a predefined threshold, an attack is predicted. This adaptive learning framework ensures robust and dynamic detection of evolving threats in real-time IoT-edge environments. The proposed GTMLP-SRS algorithm integrates temporal behavior analysis, adaptive retraining, and dynamic thresholding to accurately detect evolving attack patterns. MLP-driven hyperparameter tuning further enhances model performance through ensemble optimization and grid-based validation.

4. EXPERIMENT SETUP AND RESULTS

The proposed GTMLP-SRS framework was implemented using Python 3 within an IoT-edge-enabled environment, where the detection model was deployed at the edge layer for real-time attack prediction. A computing environment with an Intel Core i7 processor and 16 gigabytes of memory was used to conduct experiments to ensure computational efficiency and support for model training and inference.

4.1 Dataset

Two widely recognized benchmark datasets were utilized: UNSW-NB15 [37] and ToN-IoT. The UNSW-NB15 benchmark, industrialized by the Australian Centre for Cyber Security (ACCS) consist of consists of legitimate and malicious traffic. It covers nine categories of attacks such as backdoors, worm, DoS, and, comprising 49 features relevant to network behavior analysis. The ToN-IoT dataset expands upon UNSW-NB15 by integrating telemetry, operational, and network-based logs from real-world IoT deployments. It simulates modern IoT attack scenarios and provides a comprehensive view of multi-source threats across heterogeneous IoT devices and services.

4.2 Evaluation metrics

The attack mitigation effectiveness of the GTMLP-SRS was assessed utilizing standard classification metrics, defined as follows as Eqs. (14)-(17):

$$Accuracy = \frac{TP\ + TN}{TP\ + TN\ + FP\ + FN} \tag{14}$$

$$Precision = \frac{TP}{TP + FP} \tag{15}$$

$$Recall = \frac{TP}{TP + FN} \tag{16}$$

$$F - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{17}$$

where, TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively. These evaluation metrics collectively measure how effectively the model distinguishes between malicious and legitimate activities in IoT-edge computing environments.

5. PERFORMANCE EVALUATION

This subsection reports attack mitigation outcome of the proposed GTMLP-SRS according to the evaluation metrics defined in Eqs. (10)-(12). The experimental results on the UNSW-NB15 benchmark are illustrated in Figure 4. GTMLP-SRS attained an outstanding F1-score, recall, precision, and accuracy of 99.959%, 99.973%, 99.971%, and 99.97%, respectively. The outcome attained highlight the GTMLP-SRS capability for accurately identifying malicious activity while minimizing false positives and ensuring comprehensive detection of true attacks. The GTMLP-SRL robustness is further enhanced by the statistical monitoring technique employed, as described in Eq. (11), which contributes to improved detection accuracy through adaptive retraining. Similarly, performance on the ToN-IoT benchmark is presented in Figure 5, where the GTMLP-SRS model attained an outstanding F1-score, recall, precision, and accuracy of 99.89%, 99.88%, 99.91%, and 99.931%, respectively. The outcome confirms the model's reliability and adaptability to evolving attack behaviors in dynamic IoT environments. The statistical test-based retraining mechanism ensures that the model remains effective even as attack patterns shift over time, thereby supporting a resilient and secure IoT-edge infrastructure.

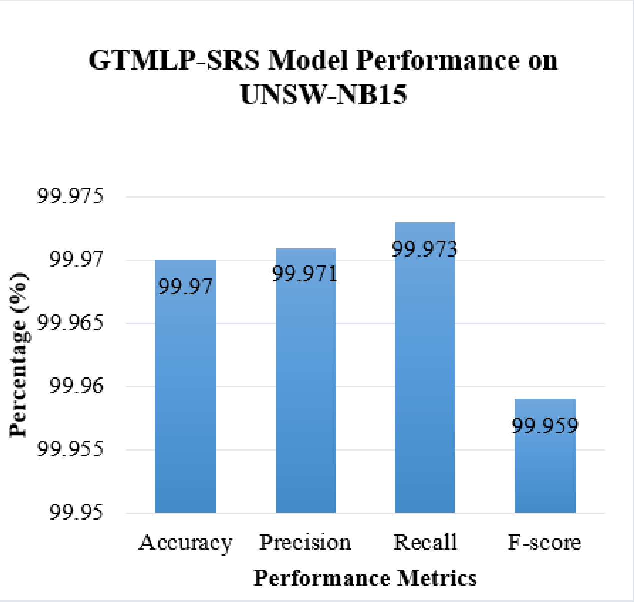


Figure 4. Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security (GTMLP-SRS) performance on University of New South Wales – Network Behavior 2015 Dataset (UNSW-NB15) dataset

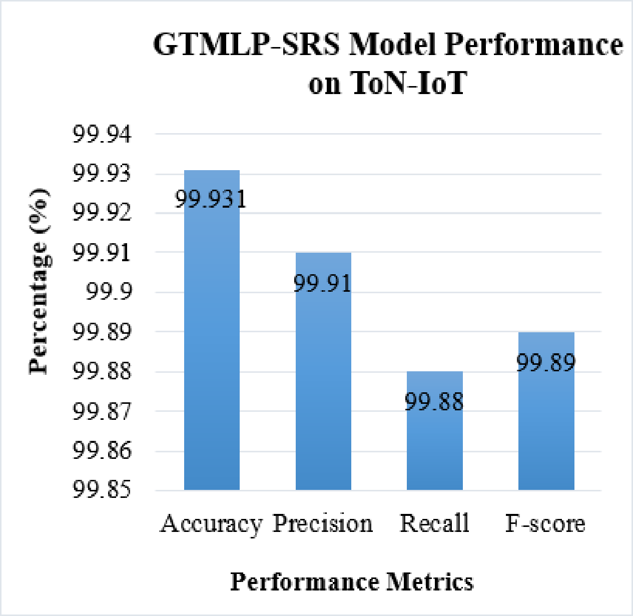


Figure 5. GTMLP-SRS performance on Telemetry over Network–Internet of Things (ToN-IoT) dataset

5.1 Comparative study on Telemetry over Network–Internet of Things

To demonstrate the effectiveness of the proposed GTMLP-SRS framework, in this work provided experimental study using the widely accepted ToN-IoT benchmark. The model's performance was compared with recent IDS-CPS frameworks, including both classical and artificial intelligence-based approaches. The evaluation metrics included F1-score, recall, precision, and accuracy, as briefed in Table 2. Table 2 clearly illustrates that the GTMLP-SRS superiorly outdoes all baseline methodologies across all evaluation metrics: GTMLP-SRS achieves an F1-score, recall, precision, and accuracy of 99.89%, 99.88%, 99.91%, and 99.931%, respectively, which are the highest across all models compared. The closest competing approach, Bi-GRU-LSTM [20], reports an accuracy of 99.55%, which is approximately 0.38% lower than GTMLP-SRS. While marginal, this improvement is critical in intrusion detection scenarios where even a small percentage can translate into significantly fewer undetected threats. Compared to classical hybrid techniques such as CAARQA [2] and GADAD-ET [18], the proposed model delivers an absolute accuracy gain of 1.1% to 4.93%, showcasing its robustness against traditional optimization-based IDS frameworks. The MV-AE-CNN [24] model demonstrates an F1-score of only 92.5%, despite a reported accuracy range of 98.7%–99.1%, indicating an inconsistency in classification performance, particularly under class imbalance and dynamic pattern, an issue effectively handled by GTMLP-SRS. The proposed GTMLP-SRS not only achieves significant results on the ToN-IoT benchmark but also demonstrates strong generalization capability, precision-recall balance, and architectural efficiency. These qualities make it a promising candidate for real-time and scalable deployment in IoT-based cybersecurity applications.

5.2 Comparative study UNSW-NB15

To further validate the generalizability and robustness of the proposed GTMLP-SRS framework, we evaluated its performance on the UNSW-NB15 benchmark which is widely adopted for IDS evaluation. The model's results were compared against several contemporary approaches from recent literature, as shown in Table 3. The results interpretate, the GTMLP-SRS outperforms all competing models across every evaluation metric: GTMLP-SRS attained F1-score, recall, precision, and accuracy of 99.959%, 99.973%, 99.971%, and 99.97%, respectively, core of establishing a new performance benchmark on the UNSW-NB15 benchmark. Compared to GNNAD [21], the most competitive baseline (accuracy: 98.84%), the GTMLP-SRS framework yields an absolute accuracy improvement of 1.13%, demonstrating its enhanced capability in detecting complex attack patterns inherent in the dataset. MV-AE-CNN [24] reports an F1-score of only 85.6%, indicating reduced consistency despite a high accuracy range (97.9%–98.5%), which highlights its potential vulnerability to class imbalance and false positive rates, limitations effectively addressed by GTMLP-SRS. Classical ensemble and semi-supervised approaches, such as SSL-RF [25] and ReMeNet [27], exhibit significantly lower performance across all metrics, with accuracies ranging from 81.1% to 91.7%, which underscores the limited adaptability of conventional models to the highly dynamic nature of modern intrusion patterns. Notably, TRACER [26] and GMCWAE [28] fall behind with accuracies of 86.02% and 81.1%, respectively, highlighting their restricted generalization and scalability for detecting threats in diverse IoT-CPS and industrial atmospheres. The experimental findings on the UNSW-NB15 benchmark reaffirm the effectiveness of the GTMLP-SRS framework. It consistently outperforms current cyber-threat detection methodologies in both detection accuracy and overall classification effectiveness. These results validate its capability for realistic deployment in high-assurance and performance-sensitive IoT security environments.

Table 2. GTMLP-SRS performance comparison with existing approaches using the Telemetry over Network-IoT (ToN-IoT) dataset

Model and References	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
CAARQA [2]	98.83	98.56	98.81	98.65
GADAD-ET [18]	95	95	95	94
LSTM-ResNet [19]	99.24	99.18	99.15	99.16
Bi-GRU-LSTM [20]	99.55	99.31	99.24	99.39
GNNAD [21]	97.67	98.21	97.67	97.84
ST-LSTM [23]	98.8	98.24	98.67	98.45
StatAvg [22]	93.38	-	-	61.22
MV-AE-CNN [24]	98.7–99.1	-	-	92.5
GTMLP-SRS [Proposed]	99.931	99.91	99.88	99.89

Note: CAARQA: Capsule Networks, Attention Augmented–Recurrent Neural Network, Quantum-based Particle Swarm Optimization, and Adaptive Neuro–Fuzzy system; GADAD-ET: Genetic Algorithm–Driven Anomaly Detector with Ensemble Tree; LSTM: Long Short-Term Memory; Bi-GRU-LSTM: Bidirectional Gated Recurrent Unit–LSTM; GNNAD: Graph Neural Network for Anomaly Detection; ST-LSTM: Swin Transformer–Long Short-Term Memory; MV-AE-CNN: Multi-View Auto-Encoder Convolutional Neural Network; GTMLP-SRS: Gradient Tree Multi-Layer Perceptron–Aware Secure and Reliable Security.

Table 3. GTMLP-SRS performance comparison with existing approaches using UNSW-NB15 benchmark

Model and References	Accuracy (%)	Precision (%)	Recall (%)	F-Score (%)
LSTM-ResNet [19]	89.23	883.83	87.77	88.25
GNNAD [21]	98.84	98.8	98.84	98.78
MV-AE-CNN [24]	97.9–98.5	-	-	85.6
SSL-RF [25]	90.43	87.69	83.12	-
TRACER [26]	86.02	-	-	-
ReMeNet [27]	91.7	-	-	-
GMCWAE [28]	81.1	-	-	-
GTMLP-SRS	99.97	99.971	99.973	99.959

Note: SSL-RF: Semi-Supervised Learner–Random Forest; GMCWAE: Generative Memory-Conditioned Wasserstein Autoencoder; UNSW-NB15: University of New South Wales – Network Behavior 2015 Dataset; TRACER: Tactical Reconnaissance Armoured Combat Equipment Requirement; ReMeNet: Residual Memory Network.

Table 4. GTMLP-SRS performance comparison with existing approaches using the ToN-IoT dataset

Dataset	Compared Model	Mean Accuracy (%)	Std. Dev. (%)	Test Used	p-value	Significance
ToN-IoT	Bi-GRU-LSTM [20]	99.55	0.21	Paired t-test	< 0.01	Significant
ToN-IoT	LSTM-ResNet [19]	99.24	0.27	Paired t-test	< 0.01	Significant
UNSW-NB15	GNNAD [21]	98.84	0.32	Paired t-test	< 0.01	Significant
UNSW-NB15	MV-AE-CNN [24]	98.21	0.41	Paired t-test	< 0.01	Significant
—	GTMLP-SRS (Proposed)	99.93/99.97	0.08	—	—	—

5.3 Statistical significance and real-world impact discussion

To strengthen the comparative evaluation, a paired statistical significance test was conducted between GTMLP-SRS and the most competitive baseline models on both ToN-IoT and UNSW-NB15 benchmarks. As shown in Table 4, the obtained p values are consistently below 0.01, confirming that the observed performance improvements are statistically significant and not due to random variation.

Although the absolute accuracy improvement of 0.3–0.5% may appear marginal, its real-world impact is substantial in large-scale IoT deployments. In high-throughput CPS-IoT environments processing millions of packets daily, such an improvement can translate into thousands of additional attack instances correctly detected, significantly reducing missed intrusions and false negatives. This enhancement directly improves service availability, data integrity, and operational safety, particularly in mission-critical applications such as smart grids, healthcare monitoring, and industrial automation. The results therefore demonstrate both the statistical robustness and practical relevance of the proposed GTMLP-SRS framework.

6. CONCLUSION

The rapid expansion of the IoT has significantly enhanced the capabilities of CPS by tightly coupling smart devices with edge and cloud infrastructures. However, this evolution has simultaneously introduced complex and highly dynamic security threats that challenge conventional intrusion detection systems. In this work, we proposed a novel adaptive intrusion detection framework, GTMLP-SRS, which tightly integrates gradient-tree optimized multi-layer perceptron learning with a statistical residual shift monitoring mechanism. Unlike traditional AI-based IDS models, GTMLP-SRS explicitly detects behavioral deviations and dynamically adapts to evolving attack patterns, enabling robust detection under non-stationary and concept-drifting environments. Extensive experiments conducted on the UNSW-NB15 and ToN-IoT benchmarks demonstrate that the proposed model consistently outperforms state-of-the-art IDS frameworks, achieving 99.97% and 99.931% detection accuracy, respectively, while maintaining a strong precision–recall balance and minimal false positives. These results confirm the effectiveness, adaptability, and scalability of GTMLP-SRS for securing IoT-Edge-Cloud CPS infrastructures. As future work, we plan to extend GTMLP-SRS into an ensemble-based adaptive IDS by integrating complementary deep learning architectures to further improve resilience against severe class imbalance and complex attack distributions. The framework will be evaluated on Internet of Vehicles (IoVs) datasets to assess mobility-aware threat detection. Additionally, we aim to incorporate federated learning to enable privacy-preserving, decentralized training across distributed edge nodes. Finally, real-world deployment trials on resource-constrained edge devices will be conducted to evaluate latency, energy efficiency, and scalability, moving the proposed framework closer to practical, large-scale CPS security deployment.

ACKNOWLEDGEMENT

The authors would like to express their sincere appreciation to all individuals who contributed to and supported this research. In particular, the authors gratefully acknowledge their supervisor for his invaluable guidance, constructive feedback, and continuous support throughout the course of this study.

REFERENCES

[1] Eren, K.K., Küçük, K., Özyurt, F., Alhazmi, O.H. (2025). Simple yet powerful: Machine learning-based IoT intrusion system with smart preprocessing and feature generation rivals deep learning. IEEE Access, 13: 41435-41455. https://doi.org/10.1109/ACCESS.2025.3547642

[2] Logeswari, G., Roselind, J.D., Tamilarasi, K., Nivethitha, V. (2025). A comprehensive approach to intrusion detection in IoT environments using hybrid feature selection and multi-stage classification techniques. IEEE Access, 13: 24970-24987. https://doi.org/10.1109/ACCESS.2025.3532895

[3] Andriulo, F.C., Fiore, M., Mongiello, M., Traversa, E., Zizzo, V. (2024). Edge computing and cloud computing for internet of things: A review. Informatics, 11(4): 71. https://doi.org/10.3390/informatics11040071

[4] Arcas, G.I., Cioara, T., Anghel, I., Lazea, D., Hangan, A. (2024). Edge offloading in smart grid. Smart Cities, 7(1): 680-711. https://doi.org/10.3390/smartcities7010028

[5] Ismail, S., Dandan, S., Qushou, A.A. (2025). Intrusion detection in IoT and IIoT: Comparing lightweight machine learning techniques using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset datasets. IEEE Access, 13: 73468-73485. https://doi.org/10.1109/ACCESS.2025.3554083

[6] Sahu, S.K., Mazumdar, K. (2024). Exploring security threats and solutions techniques for Internet of Things (IoT): From vulnerabilities to vigilance. Frontiers in Artificial Intelligence, 7: 1397480. https://doi.org/10.3389/frai.2024.1397480

[7] Wang, H., Kandah, F., Mendis, T., Medury, L. (2025). Clustering-based intrusion detection system meets multi-critics generative adversarial networks. IEEE Internet of Things Journal, 12(11): 16112-16128. https://doi.org/10.1109/JIOT.2025.3533918

[8] Singh, N., Buyya, R., Kim, H. (2024). Securing cloud-based internet of things: Challenges and mitigations. Sensors, 25(1): 79. https://doi.org/10.3390/s25010079

[9] Uddin, R., Kumar, S.A., Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks, 152: 103322. https://doi.org/10.1016/j.adhoc.2023.103322

[10] Mahadevappa, P., Al-Amri, R., Alkawsi, G., Alkahtani, A.A., Alghenaim, M.F., Alsamman, M. (2024). Analyzing threats and attacks in edge data analytics within IoT environments. IoT, 5(1): 123-154. https://doi.org/10.3390/iot5010007

[11] Yaras, S., Dener, M. (2024). IoT-based intrusion detection system using new hybrid deep learning algorithm. Electronics, 13(6): 1053. https://doi.org/10.3390/electronics13061053

[12] Priyadarshini, I. (2024). Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning. Big Data and Cognitive Computing, 8(3): 21. https://doi.org/10.3390/bdcc8030021.

[13] Saiyedand, M.F., Al-Anbagi, I. (2024). Deep ensemble learning with pruning for DDoS attack detection in IoT networks. IEEE Transactions on Machine Learning in Communications and Networking, 2: 596-616. https://doi.org/10.1109/TMLCN.2024.3395419

[14] Alshehri, M.S., Saidani, O., Alrayes, F.S., Abbasi, S.F., Ahmad, J. (2024). A self-attention-based deep convolutional neural networks for IIoT networks intrusion detection. IEEE Access, 12: 45762-45772. https://doi.org/10.1109/ACCESS.2024.3380816

[15] Abd Elaziz, M., Fares, I.A., Aseeri, A.O. (2024). Ckan: Convolutional Kolmogorov–Arnold networks model for intrusion detection in IoT environment. IEEE Access, (12): 134837-134851. https://doi.org/10.1109/ACCESS.2024.3462297

[16] Chandnani, C.J., Agarwal, V., Kulkarni, S.C., Aren, A., Amali, G.B., Srinivasan, K. (2025). A physics based hyper parameter optimized federated multi-layered deep learning model for intrusion detection in IoT networks. IEEE Access, 13: 21992-22010. https://doi.org/10.1109/ACCESS.2025.3535952

[17] Berguiga, A., Harchay, A., Massaoudi, A. (2025). HIDS-IoMT: A deep learning-based intelligent intrusion detection system for the internet of medical things. IEEE Access, 13: 32863-32882. https://doi.org/10.1109/ACCESS.2025.3543127

[18] Saiyed, M.F., Al-Anbagi, I. (2024). A genetic algorithm- and t-test-based system for DDoS attack detection in IoT networks. IEEE Access, 12: 25623-25641. https://doi.org/10.1109/ACCESS.2024.3367357

[19] Cui, B., Chai, Y., Yang, Z., Li, K. (2024). Intrusion detection in IoT using deep residual networks with attention mechanisms. Future Internet, 16(7): 255. https://doi.org/10.3390/fi16070255

[20] Javeed, D., Gao, T., Saeed, M.S., Kumar, P. (2023). An intrusion detection system for edge-envisioned smart agriculture in extreme environment. IEEE Internet of Things Journal, 11(16): 26866-26876. https://doi.org/10.1109/JIOT.2023.3288544

[21] Yang, C., Wu, L., Xu, J., Ren, Y., Tian, B., Wei, Z. (2024). Graph learning framework for data link anomaly detection. IEEE Access, 12: 114820-114828. https://doi.org/10.1109/ACCESS.2024.3445533.

[22] Bouzinis, P.S., Radoglou-Grammatikis, P., Makris, I., Lagkas, T., Argyriou, V., et al. (2025). Statavg: Mitigating data heterogeneity in federated learning for intrusion detection systems. IEEE Transactions on Network and Service Management, 22(4): 2944-2955.

https://doi.org/10.1109/TNSM.2025.3564387

[23] Fares, I.A., Abdellatif, A.G., Abd Elaziz, M., Shrahili, M., et al. (2025). Deep transfer learning based on hybrid swin transformers with LSTM for intrusion detection systems in IoT environment. IEEE Open Journal of the Communications Society, 6: 4342-4365. https://doi.org/10.1109/OJCOMS.2025.3569301

[24] Li, M., Qiao, Y., Lee, B. (2025). A comparative analysis of single and multi-view deep learning for cybersecurity anomaly detection. IEEE Access, 13: 83996-84012. https://doi.org/10.1109/ACCESS.2025.3564066

[25] Li, J., Sun, H., Du, H., Li, L., Zhang, Z. (2025). Network intrusion detection method based on semi-supervised learning and random forest. IEICE Transactions on Communications, E108-B(10): 1152-1163. https://doi.org/10.23919/transcom.2024EBP3204

[26] Wu, M., Zheng, Y., Wong, D. S. H., Wang, Y., Hu, X. (2025). TRACER: Attack-aware divide-and-conquer transformer for intrusion detection in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 21(6): 4924-4934. https://doi.org/10.1109/TII.2025.3547050

[27] Wang, X., Ma, L., Das, S.K., Liu, Z. (2025). ReMeNet: A memory-enhanced GAN model for intrusion detection in transportation cyber-physical systems. IEEE Transactions on Intelligent Transportation Systems, 26(9): 14264-14276. https://doi.org/10.1109/TITS.2025.3565257

[28] Bian, D., Liu, J. (2025). GMCWAE: A representation learning technique for network intrusion detection in IoT. IEEE Internet of Things Journal, 12(12): 20343-20356. https://doi.org/10.1109/JIOT.2025.3542845

[29] Hozouri, A., Mirzaei, A., Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. Discover Artificial Intelligence, 5(1): 314. https://doi.org/10.1007/s44163-025-00578-1

[30] Zhang, Y., Muniyandi, R.C., Qamar, F. (2025). A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance. Applied Sciences, 15(3): 1552. https://doi.org/10.3390/app15031552

[31] Sadhwani, S., Khan, M.A.H., Muthalagu, R., Pawar, P.M., Suresh, K. (2025). A hybrid BiLSTM-CNN approach for intrusion detection for IoT applications. Scientific Reports. https://doi.org/10.1038/s41598-025-29079-y

[32] Ghasemi, A., Keshavarzi, A., Abdelmoniem, A.M., Nejati, O.R., Derikvand, T. (2025). Edge intelligence for intelligent transport systems: Approaches, challenges, and future directions. Expert Systems with Applications, 280: 127273. https://doi.org/10.1016/j.eswa.2025.127273

[33] Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. Sensors, 25(1): 213. https://doi.org/10.3390/s25010213

[34] Sridharan, S., Patil, S., Shobha, T., Pai, P. (2025). Hybrid machine learning–based intrusion detection for zero-day attack prevention in digital education networks. International Journal of Safety & Security Engineering, 15(8): 1703-1713. https://doi.org/10.18280/ijsse.150815

[35] Kurian, J.F., Allali, M. (2024). Detecting drifts in data streams using Kullback-Leibler (KL) divergence measure for data engineering applications. Journal of Data, Information and Management, 6(3): 207-216. https://doi.org/10.1007/s42488-024-00119-y

[36] The UNSW-NB15 Dataset | UNSW Research. https://research.unsw.edu.au/projects/unsw-nb15-dataset.

[37] The TON_IoT Datasets | UNSW Research. https://research.unsw.edu.au/projects/toniot-datasets.