**Chellaperumal MUTHUKUMARAN, PhD Candidate (corresponding author)**
cmuthukumaran77@gmail.com
K. Ramakrishnan College of Technology, Tiruchirappalli, India

**Radhakrishnan SARAVANAKUMAR, PhD**
saravanakumar24@gmail.com
CARE College of Engineering (Autonomous), Tiruchirappalli, India

**Shanmugam Ganesan SUSILA, PhD**
susilasg1980@gmail.com
Anna University, Tiruchirappalli, India

# Mitigating Anomaly-Based DDoS Attack in Heterogeneous IoT Networks with a Federated Learning Model

**Abstract.** *The rapid expansion of the Internet of Things (IoT) networks has increased vulnerability to Distributed Denial of Service (DDoS) attacks due to resource constraints, communication overhead, secure aggregation, and real-time anomaly detection. This paper proposes a Federated Learning (FL) model for mitigating DDoS attacks in large-scale heterogeneous IoT networks. The proposed model developed an FL-based approach that improves DDoS attack detection and mitigation by leveraging machine learning models like light gradient boosting machines, extreme gradient boosting, and random forest. To ensure secure aggregation, we used homomorphic encryption and reduced communication overhead by compression techniques. Furthermore, real-time anomaly detection is achieved using a hybrid model that integrates signature-based and anomaly-based detection. After comparing it with the existing models, the proposed model demonstrates outstanding performance across various metrics. According to simulation results, the proposed model attained an accuracy of 99.80%, which signifies its efficiency in providing security in IoT networks.*

**Keywords:** *Anomaly-based detection model, DDoS attack detection, Federated Learning, Hybrid detection model, IoT networks, lightweight model, Secure aggregation.*

**JEL Classification:** C80, C81, C88.

| Received: 17 April 2025 | Revised: 21 April 2025 | Accepted: 10 September 2025 |
|---|---|---|

## 1. Introduction

The Internet of Things (IoT) has revolutionised the world in the last ten years. Millions of devices are interconnected by utilising IoT technology, whether real or digital (Jahangeer et al., 2023). It has become widely used in academia and industry, and the industrial modernisation of IoT will soon involve billions of heterogeneous devices. Excessively, the IoT-based prediction of a large-scale implementation faces significant obstacles in numerous areas (Noaman et al., 2022). Many cyberattacks have evolved significantly, ranging from traditional Denial-of-Service (DoS) and

DOI: 10.24818/18423264/59.3.25.11

Distributed DoS (DDoS) attacks to sophisticated exploits such as phishing, malware, Structured Query Language (SQL) injection, and data exfiltration. Understanding these attack types is crucial for designing effective Intrusion Detection Systems (IDS) (Abed et al., 2023). Distributed Denial of Service (DDoS) is the network's most frequent security risk. These attacks are effective because the botnet is their primary attack source. Various attack detection techniques have been developed to mitigate this, with differing success rates (Adedeji et al., 2023). Machine Learning (ML) and Deep Learning (DL) techniques have revealed encouraging outcomes in analysing network traffic and identifying botnet behaviour patterns (Alyazia et al., 2024).

Anomaly detection is a crucial component in identifying irregular behaviours in IoT networks, which face additional difficulties due to the heterogeneity of IoT devices and their limited computational resources (Cook et al., 2029). Various studies have focused on enhancing IoT network security, particularly against DDoS attacks. These include ML-based IDS to improve detection accuracy (Sadhwani et al., 2023). DL frameworks and cloud-based security measures like Moving Target Defense (MTD) and Simple Network Management Protocol (SNMP) were employed to reduce attack risks (Gayathri et al., 2023). FL models were developed to improve privacy and efficiency. In contrast, hybrid models have combined techniques like KG-Synthetic Minority Oversampling Technique (SMOTE) and K-means clustering to reduce overfitting and increase accuracy (Lv et al., 2023). Despite these advancements in IoT networks, challenges like resource constraints, communication overhead, security, scalability, and real-time detection remain significant challenges, particularly in large-scale heterogeneous IoT networks. To overcome these, the proposed model developed a solution to mitigate DDoS attacks, enhance detection accuracy, and ensure scalability while maintaining computational efficiency in resource-constrained IoT environments.

This paper presents a few contributions to a secure IoT deployment.

- The proposed model incorporates lightweight machine-learning models such as LightGBM, XGBoost, and Random Forest (RF) to reduce computational resources.
- The model uses Federated Learning (FL) to enable distributed training across IoT devices without sharing raw data. It conserves data privacy while allowing collective learning, making it suitable for large-scale IoT networks where data privacy and security are critical.
- The proposed model integrates compression techniques such as quantisation and sparsification. These methods significantly reduce the size of updates, enhancing scalability and minimising communication latency.
- The proposed model utilises homomorphic encryption, which ensures that model updates are encrypted and cannot be intercepted or tampered with during transmission.
- The proposed model introduces a hybrid detection model that combines signature-based and anomaly-based detection for known and unknown attacks. This combination ensures continuous monitoring of the model's

performance and makes improvements based on feedback and new attack patterns.

The study is formatted in the following way: The related work of anomaly-based detection for IoT networks is analysed in Section 2; the proposed model is thoroughly explained in Section 3; the implementation of the proposed model and comparison with existing models is shown in Section 4; and in Section 5 the study is concluded.

## 2. Related Work

This section analyses the existing works of DDoS attack detection in the IoT environment. (Lee et al., 2022) created an independent defence mechanism that integrated a two-dimensional CNN (2D CNN) along with edge computing to detect and avoid DDoS attacks. The system used a trained CNN to recognise DDoS attacks by investigating packet traffic and achieved high accuracy in distinguishing normal and attack traffic. However, it was only trained for usual DDoS attacks and could not identify new types of attacks. To address this, (Ogini et al., 2022) proposed a bagging-based ensemble ML model to monitor and prevent DDoS attacks in IoT environments. Although this model performed well, it still had a false positive rate, which could lead to some benign traffic being detected as malicious. To protect IoT devices from DDoS attacks, (Ibrahim et al., 2022) used a distributed Ethereum blockchain model to authenticate IoT devices. The model eliminated a single point of failure and third-party dependencies, but faced scalability and resource constraint issues. Similarly, (Aslam et al., 2022) developed a system for finding and reducing the effect of DDoS attacks using an adaptive ML-based Software Defined Network (SDN) enabled by a multi-layered feed-forwarding approach and Ensemble Voting (EV) algorithm. The framework provided high accuracy in DDoS detection, low false alarm rates, and efficient resource management. However, it further required extensive computational resources for real-time traffic analysis. These challenges were partially reduced by (Mahadik et al., 2024), which developed an Edge-FL-based IDS to protect heterogeneous IoT applications from DDoS attacks. With the DL-based one-dimensional CNN (1D-CNN) and CICDDoS2019 dataset, this model outperformed in detecting DDoS attacks while achieving high accuracy and preserving data privacy. However, this work too faced scalability issues due to communication overhead.

Using fully connected deep four-layer networks, (Awajan, 2023) developed a DL-based IDS for IoT networks. The model achieved average accuracy and demonstrated reliable performance in detecting DDoS attacks, but this model was only trained for a few types of attacks. Similarly, (Shieh et al., 2023) developed a novel IDS using CNN and geometrical metrics to detect DDoS attacks. This model achieved a high detection rate but struggled with identifying new attack patterns. To mitigate this, (Mahadik et al., 2023) aimed to develop an intelligent IDS for heterogeneous IoT environments to identify and mitigate various DDoS attacks using CNN. This model achieved a high accuracy rate for binary classification, was

simple and lightweight, and was less complex. However, this work could not provide real-time detection of attacks. Existing models face several challenges in resource constraints, communication overhead, real-time anomaly detection, security vulnerabilities, and scalability in large-scale heterogeneous IoT networks. These issues hinder the effective mitigation of DDoS attacks, especially in dynamic environments. To address these issues, the proposed model introduces an innovative approach that integrates FL to mitigate DDoS attacks for large-scale heterogeneous IoT networks. By utilising FL, the model enables decentralised training and reduces communication overhead. This approach ensures security, scalability, and real-time anomaly detection in resource-constrained environments.

## 3. Proposed Federated Learning-based DDoS Attack Detection Model

The proposed model uses FL, compression techniques, and secure aggregation methods for mitigating DDoS attacks in large-scale IoT networks using the CIC-IoT-2023 dataset. The proposed model's detailed workflow is depicted in Figure 1.

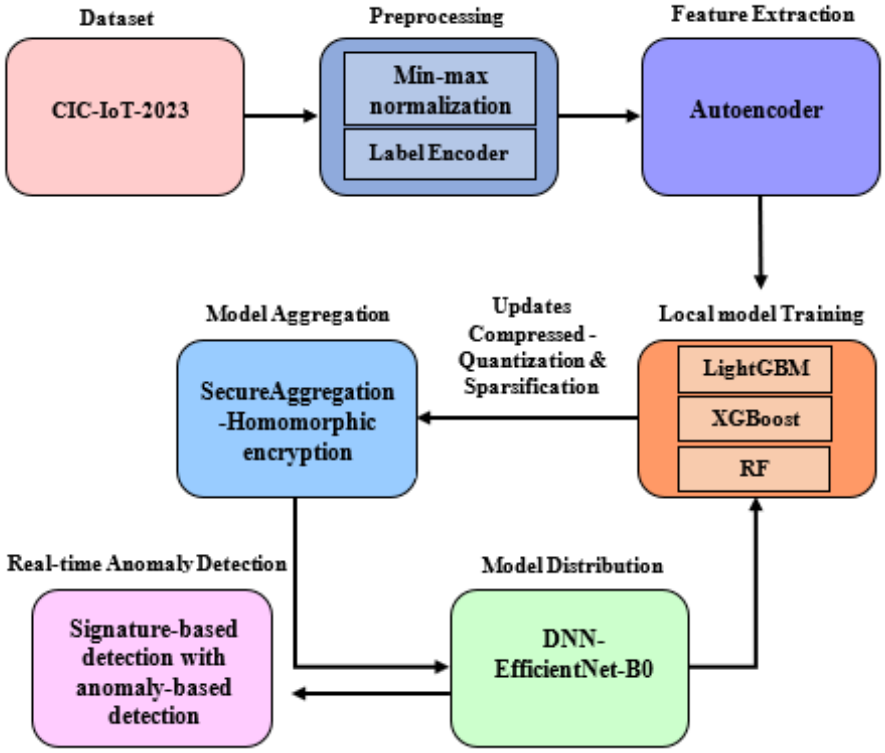


**Figure 1. The proposed FL-based model for anomaly detection in real-time**
*Source:* Authors' own creation.

### *3.1 Dataset Description*

The proposed work utilised the CIC-IoT-2023 dataset, which is recognised as the largest IoT dataset, gathered from real IoT devices. It includes data from 105 IoT devices and documents 33 recorded attacks. Notably, these attacks were carried out by malicious IoT devices targeting other IoT devices. Furthermore, the CIC-IoT-2023 dataset features multiple types of attacks that are not found in other IoT datasets. Overall, it comprises a total of 46 features and 1 label.

### *3.2 Federated Learning*

FL is an ML approach that enables model training across distributed devices or servers without changing the data. This approach differs from conventional centralised learning, which gathers data for training in a single location. Using local data, each device or server independently computes model updates and then shares them with peers or a central server. The global model improves the updates and is directed back to the devices for further development.

### *3.3 Preprocessing*

Preprocessing is an important task in data analysis. It improves the quality and reliability of the data, which in turn enhances the accuracy and optimises the performance of the dataset.

**Min-Max Normalisation:** The proposed model applies min-max normalisation for scaling the data features in the range [0, 1].

**Label Encoding:** Label encoding converts categorical variables into numerical values for each column. This ensures that the data within each column is compatible with ML algorithms.

### *3.4 Feature Extraction using AutoEncoder*

The AE is an unsupervised neural network composed of two parts: the encoder and the decoder. The encoder maps the original input into a hidden space layer, while the decoder is responsible for recreating the original input from the hidden space layer. For encoding, the training involves initialising the $W$ matrix and $b$ vector. Updating both using the error value $L$ as shown in Equations (1) and (2).

$$W = W + L \tag{1}$$

$$b = b + L \tag{2}$$

For decoding, convert the $\widehat{W}$ matrix and $\hat{b}$ vector to transpose $T$ of the encoder weight and bias vector $n$ as shown in Equations (3) and (4).

$$\widehat{W} = W_n^T \tag{3}$$

$$\hat{b} = b_n^T \tag{4}$$

An encoder is a probabilistic mapping function $E(u)$ that transforms an input vector $u$ into a hidden representation $h$ known as an encoder, as shown in Equations (5) and (6).

$$h = E(u) = \varphi(W\,u + b) \tag{5}$$

$$\sigma(W\,u + b) = \frac{1}{1 + e^{-(W\,u+b)}} \tag{6}$$

Where $\varphi$ is the activation function of the $W$ and $b$ matrix-vector in the encoder, $\sigma$ represents the sigmoid function that maps the input values, and $e$ is the base of the natural algorithm. A decoder is a mapping function of $D(h)$ is used to transform the reconstructed input space vector $r$ from the latent representation $h$, and decoder mapping it with a sigmoid function as stated in Equations (7) and (8).

$$r = D(h) = \varphi\left(\hat{W}\,h + \hat{b}\right) \tag{7}$$

$$\sigma\left(\hat{W}\,h + \hat{b}\right) = \frac{1}{1 + e^{-(\hat{W}\,h+\hat{b})}} \tag{8}$$

The learning process often includes optimising the weights to minimise the reconstruction error. Hence, Equation (9) expresses the objective function.

$$L = |u - \hat{u}|^2 \tag{9}$$

Where $u$ denotes an input value and $\hat{u}$ is the output value.

### *3.5 Local Model Training*

In FL, local models are trained using locally available data through traditional ML algorithms. The proposed model utilised ML algorithms such as LightGBM, XGBoost, and RF for local model training.

#### *3.5.1 LightGBM*

LightGBM is employed to train individual local models within the FL framework. By leveraging its Gradient-Boosting Decision Tree (GBDT). It enables clients to learn patterns independently from their data while preserving privacy. LightGBM utilises classification and regression trees as weak learners, iteratively refining model predictions by minimising the residual error of the previous tree. The loss minimisation process $E_R(P)$ is expressed as shown in Equation (10).

$$E_R(P) = \sum_{r=1}^{R} \lambda_r d(Q_i; \theta_r) \tag{10}$$

Where $R$ represents the number of trees, $r$ number of iterations, $\lambda_r$ represents the learning rate, $d(Q_i; \theta_r)$ represents the $r$th tree decision trees, and $\theta_r$ represents the tree parameter. The successive $r$th trees are trained to predict the residual error by minimising the loss function $\mathcal{L}$ concerning the tree parameter $\theta_r$ is shown in Equation (11).

$$\theta_r = argmin \sum_{i=1}^{n} \mathcal{L}\left(P_i, f_{r-1}(Q_i) + \lambda_r d(Q_i; \theta)\right) \tag{11}$$

Here $P_i$ represents the target variable, $f_{r-1}(Q_i)$ represents the previous tree prediction, and $n$ represents the training samples. Optimisation was performed using gradient descent, which ensures that the residuals are minimised at each iteration, enhancing the model's performance.

*3.5.2 XGBoost*

XGBoost is employed to train individual local models within the FL framework. It is a scalable and computationally efficient implementation of GBDT that builds models incrementally. For local model training, XGBoost incrementally builds an ensemble of decision trees that work together to refine predictions. The model focuses on iteratively correcting the errors of previous trees, allowing it to improve performance over time.

Each decision tree is built to minimise the residual errors of the previous one, ensuring that the model can capture complex patterns, even in noisy data. To further increase robustness against noise and overfitting, a random sampling strategy known as stochastic gradient boosting has been incorporated. XGBoost represents an enhanced implementation that employs regularisation techniques to reduce the risk of overfitting. Equation (12) is the objective function for XGBoost that needs to be minimised.

$$Obj\ func^{w} = \sum_{a=1}^{n}\left(h_a - \left(\widehat{h_a} + f_w\ (x_a)\right)\right) + \Delta(u) \qquad (12)$$

Where $h_a$ represents the target value, $\widehat{h_a}$ is the model's predicted value representing a sample $a$ 's predicted category label, $f_w\ (x_a)$, represents an additive decision tree model, and $\Delta(u)$ is the regularisation function. This regularisation ensures that the model improves over iterations and prevents overfitting, making it suitable for local training in environments with high-dimensional data.

*3.5.3 Random Forest*

RF is used as a local model training technique in the proposed model. RF is a supervised ML method that creates several decision trees for the prediction model by randomly selecting a subset of the available training data using bootstrap sampling. This approach increases model robustness by reducing overfitting and handling non-linear relationships between features. During training, each tree is created using a random subset of features at each decision node, ensuring diversity among the trees. The final output is obtained by aggregating the predictions of all trees in the forest, resulting in a robust, collective decision for an update. By combining multiple decision trees, each trained on different subsets of data and features, as shown in Equation (13).

$$\widehat{F_{RF}}(s) = \frac{1}{N}\ t_i(s) \qquad (13)$$

Where $\widehat{F_{RF}}(s)$ represents the combined model related to RF as a function of $s$, $t_i$ is a single decision tree regression model of $i$-th value, and $N$ is the number of features.

### *3.6 Compressed using Quantisation and Sparsification*

After training on each IoT device, the local model transmits its learned parameters to a central server, which can create significant communication overhead, especially in resource-constrained environments. To mitigate this, we apply model update compression techniques, namely quantisation and sparsification.

Quantisation reduces update sizes by using fewer bits to represent numerical values, leading to less data transfer with minimal accuracy loss. Sparsification further decreases communication requirements by sending only the most significant update values while filling the rest with zeros.

These compressed updates are sent to the central aggregator, which assembles the global model from the contributions of all clients. This approach supports efficient and scalable federated learning in resource-limited IoT settings without compromising model performance.

### *3.7 Global Model Training using Deep Neural Network*

The proposed model used a Deep Neural Network (DNN) based on EfficientNetB0 to train the global model. The DNN concept originates from research on ANN. DNNs are characterised by two or more hidden layers. They can learn more complex and abstract features than shallow ANNs. The EfficientNetB0 model has undergone a previous transfer learning process. It is a part of the CNN family and is specially designed for effective classification. The lightweight model architecture aims to enhance floating-point operation accuracy and efficiency. This is achieved by the compound scaling approach, which scales up the tenacity, breadth, and complexity of the architecture network. The EfficientNet-B0 network comprises a three-channel input image with a pixel resolution of 224*224. A compound coefficient $\partial$ is expressed in Equation (14).

$$s = \alpha\partial,\ q = \beta\partial,\ r = \gamma\partial \tag{14}$$

Here $\alpha \geq 1$, $\beta \geq 1$, and $\gamma \geq 1$ are scaling factors dependent on grid search and model scaling. The Swiss function with the input variable $i$ is defined as follows in Equation (15).

$$swiss(i) = \frac{i}{1+ e^{-\beta(i)}} \tag{15}$$

The final layer of the EfficientNet-B0 architecture predicts the final output based on the data removed from the preceding layers.

### *3.8 Secure Aggregation using Homomorphic Encryption*

Secure aggregation is essential to mitigate privacy threats in cross-device FL. It allows the central server to compute the aggregation of model updates from distributed devices without having access to individual gradients, thus maintaining user privacy. To ensure this, the proposed model utilised a HE, a cryptographic technique that allows computations to be performed over encrypted data without the need to decrypt it first. The HE is the most commonly used privacy protection mechanism in FL. For example, let us consider the message $m$.

Key Generation: $(kr, ku)$ key pair $\in k$ where $k$ represents key space. Which is highly dependent on the $k$ element.

Encryption: To encrypt, apply $kr$ on a message $m$ producing a ciphertext $c$ in the cipher-space.

Decryption: To decrypt, apply $ku$ on the encrypted message $c$ to produce $m$.

Mathematical operations like summation, multiplication, and logic-exclusive OR (XOR) operations could be supported by HE. This property ensures that model updates can be securely aggregated without revealing individual client information, thus enhancing the privacy-preserving capability of the FL framework.

### *3.9 Model Distribution*

In FL, the training model on data sources is distributed among edge devices. Each device is trained on its local data to ensure all clients receive the global model. Then, it performs local training and shares its updates back to the central server for aggregation.

### *3.10 Real-time Anomaly Detection*

The proposed model utilised a hybrid detection model based on the signature with anomaly-based detection to detect anomalies in real-time. The input data is filtered using statistical features in the signature anomaly detection technique. The normal data standard deviation includes a sequence of time series, which is used to filter the malicious data $(t_1, t_2, \dots)$ where $w_{i,1}, w_{i,2}, \dots, w_{i,n}$ are the individual components of the vector $t_i$ is sampled at a time interval $i$. Each $t_i$ is composed of $n$ elements as shown in Equation (16).

$$t_i = w_{i,1}, w_{i,2}, \dots, w_{i,n} \tag{16}$$

where $n$ is the dataset's total number of sensors and actuators. Let $M$ be the length $v$ of a data segment $m_{T+1}, \dots., m_{T+v-1}$ at a specific time $T$ as defined in Equation (17).

$$M = (m_T, m_{T+1}, \dots., m_{T+v-1}) \tag{17}$$

Where $v$ is the window size. The training phase of $n$ standard deviation $SD_1, SD_2, \dots, SD_n$ are calculated for each possible segmented normal data as represented in Equation (18).

$$SD_j = \varphi\left(w_{T,j}, w_{T+1,j}, \dots, w_{T+v-1,j}\right) \quad (18)$$

The standard deviation $SD_j$ of $v$ consecutive values $w_{T,j}, w_{T+1,j}, \dots, w_{T+v-1,j}$ for the $j$-th sensor or actuators. Then, for each potential case, the minimum and maximum standard deviations are calculated in Equations (19) and (20).

$$Min_{SD_j} = min\, SD_j \quad (19)$$

$$Max_{SD_j} = max\, SD_j \quad (20)$$

Where $Min_{SD_j}$ and $Max_{SD_j}$ are the standard deviations lower and upper bounds $v$ normal reported values for sensors or actuators correspondingly. When a test input segment $S_i$ of $v$ consecutive samples $t_i, t_{i+1}, \dots, t_{i+v-1}$ from Equation (21) is processed, the method computes a Boolean predicate $R_1, R_2, \dots, R_n$ where each $R_j$ as True or False

$$S_i = t_i, t_{i+1}, \dots, t_{i+v-1} \quad (21)$$

When labeled normal, the input moves to the next iteration, finding a stage to reduce false negatives. The model adapts to diverse attack patterns by leveraging a dynamic threshold mechanism. The input error is classified as anomalous if it exceeds a predefined threshold. The model adjusts its threshold over time by incorporating feedback from detected anomalies and periodic retraining with updated datasets. This ensures its adaptability to changing patterns in real-world IoT environments.

## 4. Results and Discussions

The proposed FL model's performance analysis is in this section. The experiment was conducted on a GPU: NVIDIA Quadro, CPU: Intel® Xeon® CPU E5-1650v3@3.50GHz M2000, Python 3.10 x64-based processors, and the 64-bit Windows 10 Pro operating system.

### *4.1 Performance Analysis of the Proposed Model*

Table 1 illustrates the effectiveness of the locally trained model with the LightGBM, XGBoost, and RF models across various metrics like accuracy, precision, sensitivity, specificity, F1-score, and Negative Predicted Value (NPV). Additionally, the proposed model has a low tendency for mistakes, as seen by its False Positive Rate (FPR) and False Negative Rate (FNR).

**Table 1. Performance Metrics of Local Model Training**

| Local Model | Local Model 1 (LightGBM) | Local Model 2 (XGBoost) | Local Model 3 (RF) |
|---|---|---|---|
| **Accuracy (%)** | 99.86 | 99.83 | 99.82 |
| **Precision (%)** | 99.79 | 99.74 | 99.74 |

| Local Model | Local Model 1 (LightGBM) | Local Model 2 (XGBoost) | Local Model 3 (RF) |
|---|---|---|---|
| **Sensitivity (%)** | 99.79 | 99.74 | 99.74 |
| **Specificity (%)** | 99.89 | 99.87 | 99.87 |
| **F1_Score (%)** | 99.79 | 99.74 | 99.74 |
| **FPR (%)** | 0.1003 | 0.1252 | 0.1278 |
| **FNR (%)** | 0.2006 | 0.2504 | 0.2557 |

*Source*: Authors' processing.

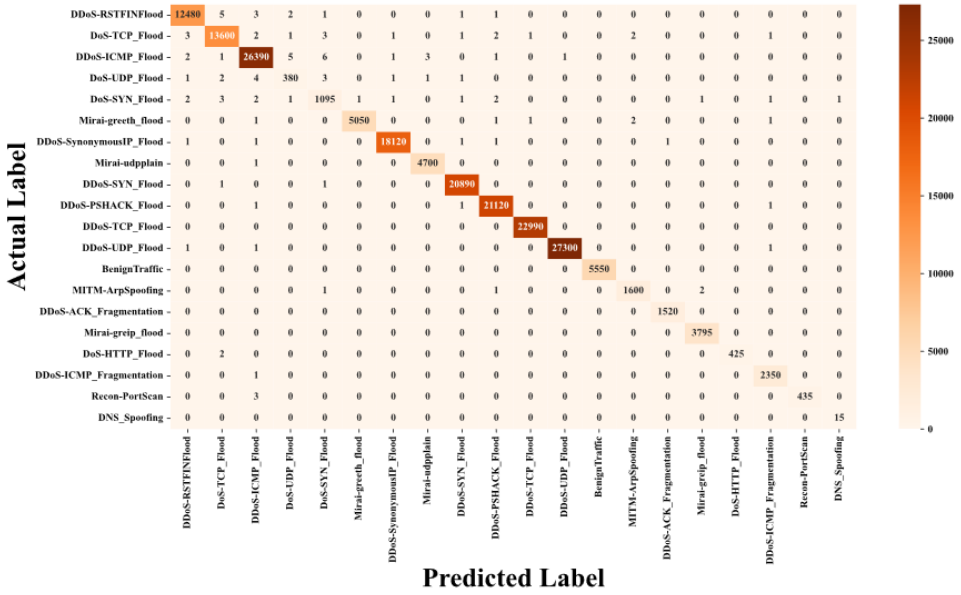


**Figure 2(a). Confusion Matrix for Local Model Trained using LightGBM**
*Source:* Authors' own creation.

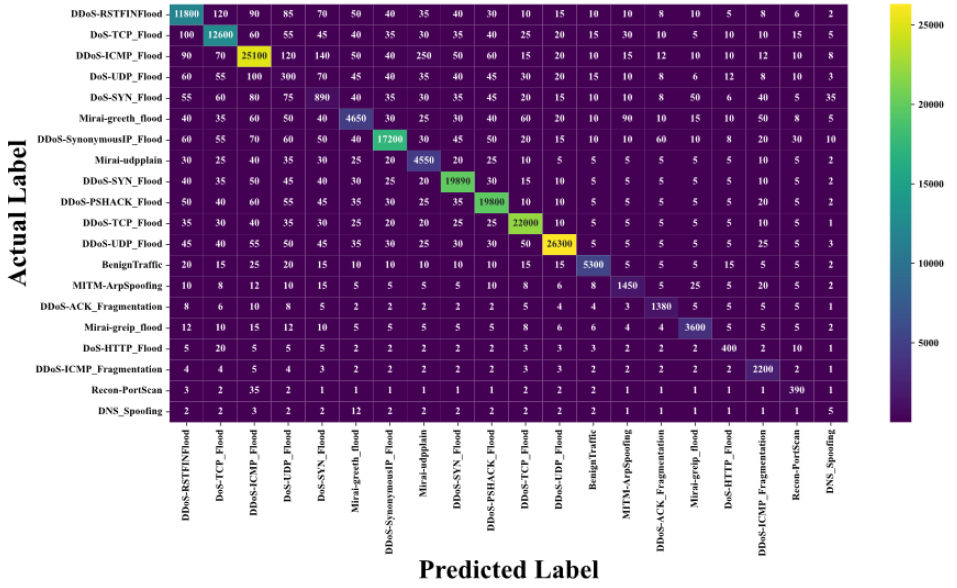


**Figure 2(b). Confusion Matrix for Local Model Trained using XGBoost**
*Source:* Authors' own creation.

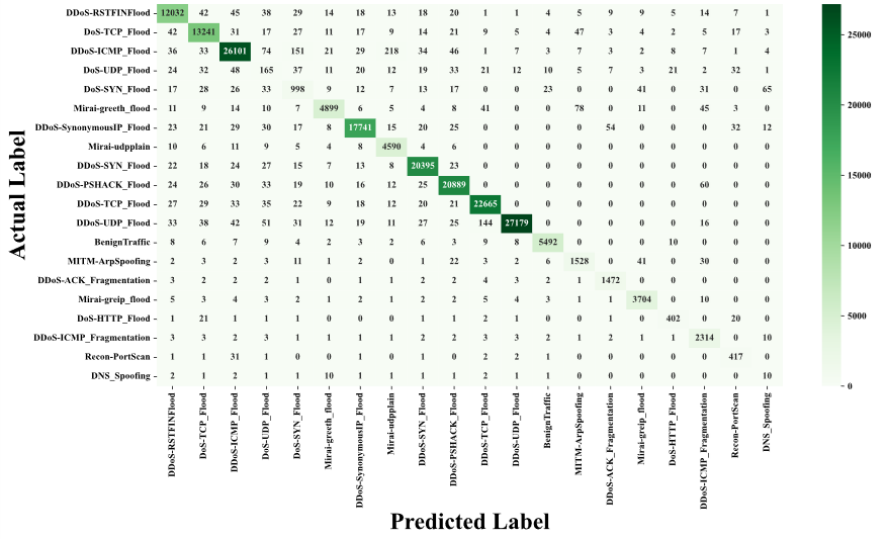


**Figure 2(c). Confusion Matrix for Local Model Trained using RF**
*Source:* Authors' own creation.

Figure 2(a-c) displays the confusion matrix for the local model training using LightGBM, XGBoost, and RF. It visualises the performance of the local model used for multi-class classification tasks involving benign, bot, and DDoS. Each row and column represented the actual and predicted values.

Table 2 illustrates the effectiveness of the worldwide model trained with EfficientNetB0 across a number of metrics, including accuracy, precision, sensitivity, specificity, and F1-score. The values of these metrics are 99.80, 99.82, 99.75, 99.85, and 99.78, respectively. Additionally, the proposed model shows a low tendency for mistakes, as seen by its FPR and FNR of 0.002 and 0.003.

**Table 2. Performance Metrics of Global Model Training**

| Global Model | EfficientNetB0 |
|---|---|
| **Accuracy (%)** | 99.8 |
| **Precision (%)** | 99.82 |
| **Sensitivity (%)** | 99.75 |
| **Specificity (%)** | 99.85 |
| **F1-score (%)** | 99.78 |
| **FPR (%)** | 0.002 |
| **FNR (%)** | 0.003 |

*Source:* Authors' processing.

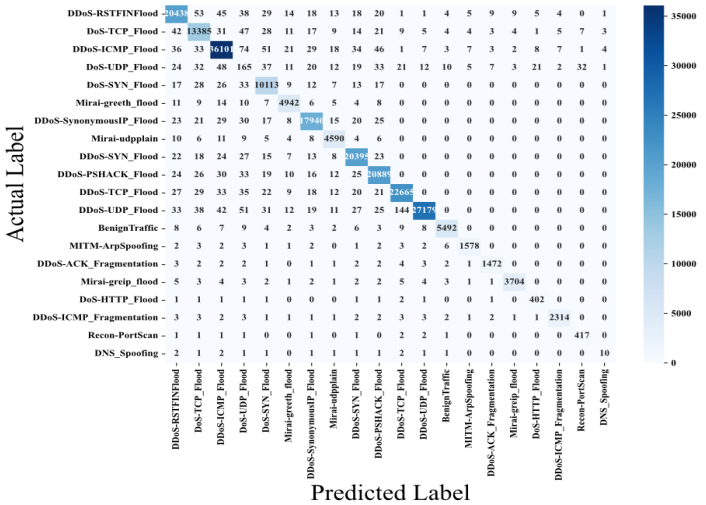


**Figure 3. Confusion Matrix for Global Model Training**
*Source:* Authors' own creation.

Figure 3 displays the confusion matrix for the global model training using EfficientNetB0. It visualises the efficiency of the global model employed in multi-class classification tasks involving benign, bot, and DDoS. Each row and column represented the actual and predicted values.

Table 3 shows that the proposed model performs exceptionally well in terms of accuracy, with low false positives and false negatives, making it highly reliable for real-world IoT environments. The considerable reduction in attack success rate and

packet loss highlights its effectiveness in mitigating DDoS attacks. Additionally, the optimised communication overhead ensures that the model is scalable and resource-efficient, which is crucial for IoT devices with limited capabilities.

**Table 3. Proposed Model Performance in Mitigating DDoS Attacks**

| Metric | Mitigation Value |
|---|---|
| Detection Accuracy | 99.80% |
| FPR | 0.10 |
| FNR | 0.25 |
| Attack Success Rate | 3.00% |
| Packet Loss During Attack | 2% |
| Communication Overhead | 0.5 MB per update |

*Source:* Authors' own creation.

### *4.2 Comparative Analysis of Proposed Model with Existing Models*

**Table 4. Comparison of performance metrics of the proposed model with existing models**

| Model | Accuracy (%) | Precision (%) | Recall (%) |
|---|---|---|---|
| LSTM [12] | 96.44 | 95.74 | 97.66 |
| 2D CNN [16] | 95.60 | 93.42 | 93.42 |
| 1D CNN [20] | 96 | 94.33 | 95.99 |
| CNN-Geo [22] | 99.70 | 99.60 | 99.40 |
| Proposed Model | 99.80 | 99.82 | 99.75 |

*Source*: Authors' own creation.

Table 4 compares the proposed model with existing models such as LSTM, CNN, 1D CNN, CNN-Geo, and Bi-LSTM. The proposed model achieved notable accuracy, precision, and recall values of 99.80, 99.82, and 99.75, respectively, outperforming the existing models.

## 5. Conclusions

In this work, we developed an innovative approach to FL-based DDoS attack mitigation in large-scale IoT networks by employing lightweight ML models like LightGBM, XGBoost, and RF instead of DL models to overcome the resource constraints of IoT devices. We integrated quantisation and sparsification techniques to reduce communication overhead to ensure efficient model updates between devices and central servers. We used HE for a secure aggregation process to prevent malicious updates and our hybrid detection model, merging signature-based and anomaly-based detection, to enable real-time anomaly detection for continuously monitoring the model's performance and improvement based on feedback and new attack patterns. The suggested model was verified utilising the CIC-IoT-2023 dataset, demonstrating its effectiveness in improving detection accuracy and

enhancing security. This approach offers a scalable and secure DDoS detection and mitigation solution in an IoT environment. Future work will focus on extending the proposed model to other types of cyber threats in IoT networks.

## References


[1] Abed, A.K., Anupam, A. (2023), *Review of security issues in Internet of Things and artificial intelligence-driven solutions. Security and Privacy*, 6(3), e285.

[2] Adedeji, K.B., Abu-Mahfouz, A.M., Kurien, A.M. (2023), *DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks*, 12(4), 51.

[3] Aldhaheri, A., Alwahedi, F., Ferrag, M.A., Battah, A. (2024), *Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and cyber-physical systems*, 4(2), 110-128.

[4] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Jilani, S.F. (2022), *Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. Sensors*, 22(7), 2697.

[5] Awajan, A. (2023), *A novel deep learning-based intrusion detection system for IOT networks. Computers*, 12(2), 34.

[6] CIC IoT Dataset 2023, (2023), https://www.kaggle.com/datasets/akashdogra/cic-iot-2023.

[7] Cook, A.A., Mısırlı, G., Fan, Z. (2019), *Anomaly detection for IoT time-series data: A survey. IEEE Internet of Things Journal*, 7(7), 6481-6494.

[8] Gayathri, R., Usharani, S., Mahdal, M., Vezhavendhan, R., Vincent, R., Rajesh, M., Elangovan, M. (2023), *Detection and mitigation of IoT-based attacks using SNMP and moving target defense techniques. Sensors*, 23(3), 1708.

[9] Ibrahim, R.F., Abu Al-Haija, Q., Ahmad, A. (2022), *DDoS attack prevention for internet of thing devices using ethereum blockchain technology. Sensors*, 22(18), 6806.

[10] Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M., Hashemi, S.H. (2023), *A review on the security of IoT networks: From network layer's perspective. IEEE Access*, 11(3), 71073-71087.

[11] Lee, S.H., Shiue, Y.L., Cheng, C.H., Li, Y.H., Huang, Y.F. (2022), *Detection and prevention of DDoS attacks on the IoT. Applied Sciences*, 12(23), 12407.

[12] Lv, H., Du, Y., Zhou, X., Ni, W., Ma, X. (2023), *A data enhancement algorithm for DDoS attacks using IoT. Sensors*, 23(17), 7496.

[13] Mahadik, S.S., Pawar, P.M., Muthalagu, R. (2024*), Edge-Federated Learning based Intelligent Intrusion Detection System for Heterogeneous Internet of things. IEEE Access*, 12(3), 81736-81757.

[14] Mahadik, S., Pawar, P.M., Muthalagu, R. (2023), *Efficient intelligent intrusion detection system for heterogeneous Internet of Things (HetIoT). Journal of Network and Systems Management*, 31(1), 2.

[15] Noaman, M., Khan, M.S., Abrar, M.F., Ali, S., Alvi, A., Saleem, M.A. (2022), *Challenges in integration of heterogeneous internet of things. Scientific Programming*, 2022(1), 8626882.

[16] Ogini, N.O., Adigwe, W., Ogwara, N.O. (2022), *Distributed denial of service attack detection and prevention model for IoT-based computing environment using ensemble machine learning approach. International Journal of Network Security & Its Applications (IJNSA)*, 14(4), 39-53.

[17] Sadhwani, S., Manibalan, B., Muthalagu, R., Pawar, P. (2023), *A lightweight model for DDoS attack detection using machine learning techniques. Applied Sciences*, 13(17), 9937.

[18] Shieh, C.S., Nguyen, T.T., Horng, M.F. (2023), *Detection of unknown ddos attack using convolutional neural networks featuring geometrical metric. Mathematics*, 11(9), 2145.