scientific reports

Check for updates

OPEN

Modelling of hybrid deep learning framework with recursive feature elimination for distributed denial of service attack detection systems

Sultan Alkhliwi

Dealing with network security has always been a challenging task, particularly in the prevention and detection of distributed denial of service (DDoS) attacks. Attacks such as DDoS pose hazards to the system by compromising its accessibility to individuals who need to use a specific server. This type of cyberattack occurs when a system is overloaded with a massive amount of traffic, causing the network to become unavailable. This attack type focuses on engaging the service with correct operators without breaching safety parameters. Responsible artificial intelligence (AI) refers to the ethical development and deployment of AI systems that prioritise fairness, transparency, privacy, and accountability. Currently, the deep learning method is very effective in distinguishing DDoS traffic from harmless traffic by removing the representation of higher-level features from lower-level traffic. The study presented in this paper proposes a responsible artificial intelligence-based hybridisation framework for attack detection using recursive feature elimination (RAIHFAD-RFE) for cybersecurity systems. The study aimed to analyse and propose efficient cybersecurity tactics for preventing, mitigating and detecting DDoS attacks using advanced methods. As a primary step, the RAIHFAD-RFE technique utilises the Z-score standardisation method for the data pre-processing phase to clean, transform and organise raw data into a structured format. Furthermore, the recursive feature elimination (RFE) model is employed for feature selection (FS) to identify and retain the most essential features, thereby improving model performance and reducing model complexity. Moreover, the hybridisation of long short-term memory and bidirectional gated recurrent unit (LSTM-BiGRU) models was employed for classification. To optimise model performance, the improved orca predation algorithm (IOPA) is utilised for hyperparameter tuning to select the optimal parameters for enhanced accuracy. A comprehensive experimental analysis of the RAIHFAD-RFE approach was performed under the CIC-IDS-2017 and Edge-industrial internet of things (IIoT) datasets. A comparison study of the RAIHFAD-RFE approach provided superior accuracy values of 99.35% and 99.39%, respectively, compared to existing models on the dual dataset.

Keywords Artificial intelligence, Applied mathematics, Distributed denial of service attack, Cybersecurity, Recursive feature elimination, Hybrid deep learning

The internet plays a vital role worldwide, serving as a global information resource for every user and making it essential. The internet is vast, providing access to data, resources and services for every domain[1]. Currently, data security is given higher importance because everything is linked to the internet. To safeguard private and personal data against malicious cyberattacks, it is crucial to implement essential measures to ensure that strong and consistent security protocols are in place[2]. As its needs increase, so do security concerns. There are numerous types of attacks affecting the internet that should be detected, identified and defended against by attackers. In particular, distributed denial of service (DDoS) is among the most prevalent assaults in cyberspace. A DDoS attack aims to utilise computing resources, thereby preventing standard work from continuing[3]. In contrast to denial of service (DoS) attacks, which do not attempt to corrupt or destroy information, DDoS attacks involve numerous resources that simultaneously assault the target systems.

Department of Computer Science, Faculty of Science, Northern Border University, Arar, Saudi Arabia. email: salkhliwi@nbu.edu.sa

DDoS attacks have become a universal and disruptive threat in the cyberworld[4]. DDoS attacks are designed to overwhelm and disable targeted systems by rendering them inaccessible to legitimate users. By overloading a website, network or online service with malicious requests or excessive traffic, DDoS attacks disrupt standard functions, causing significant disruptions, damage and financial loss to a business's reputation. DDoS assaults are noticeable in various methods, including volumetric, protocol and application layer attacks[5]. The DDoS attack is constantly evolving to keep pace with technological advances. Figure 1 illustrates the DDoS attack scenario. Attackers continually invent novel techniques to evade service provider defences driven by the development of DoS methods. As the complexity and scale of DDoS attacks continue to evolve, businesses should adopt proactive and robust defence strategies[6]. This involves applying anomaly detection (AD) and traffic monitoring methods, utilising mitigation models, and leveraging the services of specific DDoS mitigation providers. Furthermore, the effective detection and mitigation of DDoS attacks depends comprehensively on collaboration and the transfer of data between numerous entities[7].

Recently, the DL approach has been highly effective in distinguishing DDoS traffic from benign traffic by removing representations of higher-level features from those of lower-level features. The effective nature of tools in security, such as malware identification, access control, secure uploading and cloud encryption, is attained by computers and DL[8]. It is suitable for modelling nonlinear complex relations by learning numerous phases of representation that relate to several phases of abstraction. A deep neural network (DNN) comprises an array of nonlinear layers of processing units capable of conversion and feature extraction, making it a suitable method for detecting threats on social networking sites[9]. Cyberattack identification shares features that are widespread with image recognition, harnessing novel DL features. Minor variations in the pixel are inclined to recognise image variations; there, an attack is identified in the same manner as more than 99% of new threats are tiny adaptations of earlier threats. This strengthens DL's effectiveness in identifying slight variations in attack patterns. DL is implemented in cybersecurity due to its ability to self-learn and analyse[10].

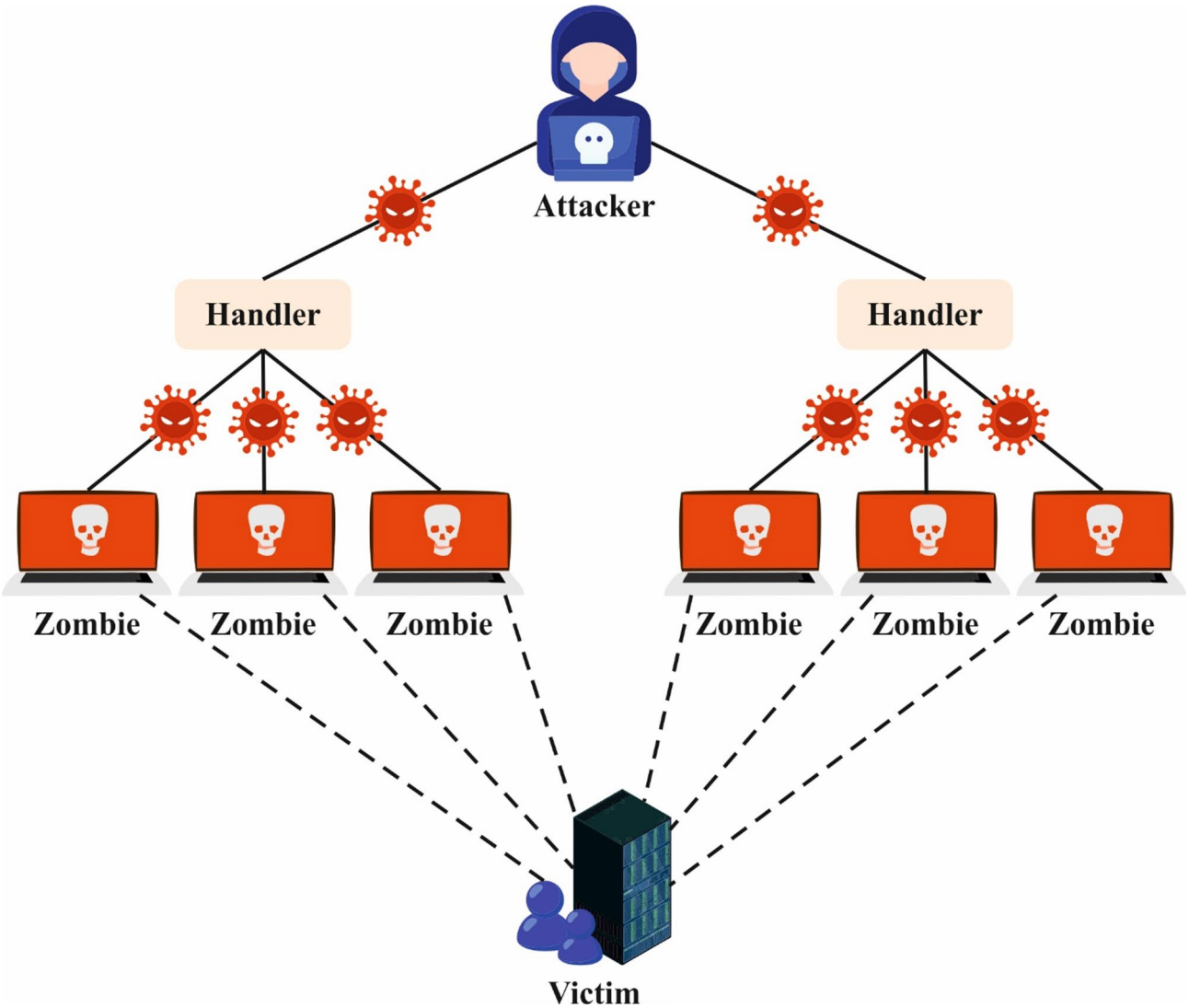

Fig. 1. DDoS attack scenario.

The study presented in this paper proposes a responsible artificial intelligence-based hybridisation framework for attack detection using recursive feature elimination (RAIHFAD-RFE) for cybersecurity systems. The study aimed to analyse and propose efficient cybersecurity tactics for preventing, mitigating and detecting DDoS attacks using advanced methods. The RAIHFAD-RFE technique utilises the Z-score standardisation method for the data pre-processing phase to clean, transform and organise raw data into a structured format. Furthermore, the recursive feature elimination (RFE) model is employed for feature selection (FS) to identify and retain the most essential features, thereby improving model performance and reducing model complexity. Moreover, the hybridisation of long short-term memory and bidirectional gated recurrent unit (LSTM-BiGRU) models was employed for classification. To optimise model performance, the improved orca predation algorithm (IOPA) is utilised for hyperparameter tuning to select the optimal parameters for enhanced accuracy. A comprehensive experimental analysis of the RAIHFAD-RFE approach was performed under the CIC-IDS-2017 and Edge-IIoT datasets. The key contribution of the RAIHFAD-RFE approach is listed below.

- The RAIHFAD-RFE model enhances pre-processing by applying Z-score standardisation to normalise input features, thereby improving learning efficiency and model convergence. This step ensures consistent feature scaling to reduce bias in training. It plays a significant role in stabilising and accelerating the overall detection process.
- The RAIHFAD-RFE method utilises the RFE technique to identify and retain the most relevant features, thereby improving the focus and interpretability of the model. This mitigates dimensionality and filters out noisy or redundant data. As a result, it improves classification accuracy and computational efficiency.
- The RAIHFAD-RFE approach integrates a hybrid LSTM-BiGRU classifier to effectively capture temporal patterns and contextual dependencies in network traffic data. This improves the accuracy and robustness of DDoS attack detection. The hybrid architecture facilitates better generalisation and learning from sequential behaviour.
- The RAIHFAD-RFE methodology utilises IOPA-based hyperparameter tuning to search intelligently for optimal parameter settings, thereby enhancing classification accuracy. This optimisation process ensures efficient model performance across a wide range of scenarios. It strengthens the adaptability and precision of the DDoS detection system.
- The integration of RFE-based feature selection (FS) with a hybrid LSTM-BiGRU classifier and IOPA-based tuning establishes a novel, responsible AI-based framework. This design uniquely integrates feature reduction, deep temporal learning and intelligent optimisation. It ensures high accuracy, efficiency and transparency in detecting DDoS attacks. The novelty lies in the unified approach to responsible, explainable and high-performance intrusion detection.

Related studies on DDoS attack detection

Alrumaih and Alenazi[11] presented a new model to enhance the resilience of industrial networks from DDoS attacks (ERINDA) to reduce downtime and uphold operations. It comprises a dual-step method that merges reactive and proactive approaches to mitigate DDoS attacks while effectively minimising network failures. Initially, network traffic is continuously examined to identify anomalies that represent probable intrusions. Next, response mechanisms are initiated in real-time threat detection to counteract the attack and reinstate network integrity rapidly. Hu and Shi[12] addressed the secure synchronisation issue for complex dynamical networks (CDNs) with an observer-enabled event-triggered communication strategy (ETCS) in multichannel DoS attacks (MCDSAs). Due to external environmental factors, viewers are expected to evaluate the network's state accurately. Wang et al.[13] proposed a framework named ARSAE-QGRU, which incorporates residual connections and attention mechanisms (AM) into a stacked autoencoder (SAE) for DDoS attack recognition. By presenting residual connections and AM in SAE, this technique efficiently transports valid data and enables the propagation of gradients, allowing for the effective learning of lower-dimensional models. Balamurugan et al.[14] improved DDoS attack detection and mitigation by utilizing the Novel Attack Detection Protocol (NADP) and comparing its performance with dynamic source routing (DSR) model. Hnamte et al.[15] proposed a groundbreaking technique to recognise DDoS attacks through a DNN framework depending on DL. This method presents an accessible and scalable model, enabling a thorough examination of network traffic data to distinguish composite formats that indicate DDoS attacks. To authenticate the method's efficiency, precise assessments were done leveraging genuine actual traffic data. The outcomes demonstrate the supremacy of this DNN-aided method compared to conventional DDoS recognition methods. Martinez et al.[16] proposed an innovative dual-space prototypical paradigm that utilises a specific dual-space function of loss to enhance recognition precision for various attack patterns as measured by angular and geometric metrics. This paradigm leverages the representation learning capabilities in the latent space, refining the paradigm's flexibility and adaptability to counter DDoS attack vectors. Ahmed et al.[17] presented a machine learning (ML)-driven trust-empowered routing protocol (TrustML-RP) model that classifies the attacking nodes accountable for packet suppression and DDoS attacks. This model implements a distributed trust model to establish trust factors between contributing nodes and then deploys an efficient integration of ML procedures, namely support vector machine (SVM) and artificial neural network (ANN), for finding the best and most secure path and identifying attacker nodes.

Hossain and Islam[18] proposed ensemble-based random forest (RF) classifier integrated with advanced feature selection techniques such as principal component analysis (PCA), mutual information (MI), and correlation analysis with the Synthetic Minority Over-sampling Technique (SMOTE) to address class imbalance. Emirmahmutoğlu and Atay[19] proposed a model to improve the performance of anomaly-based intrusion detection systems (IDS) by applying heuristic FS methods, namely particle swarm optimisation (PSO), flower pollination algorithm (FPA), and differential evolution (DE), integrated with various ML classifiers. Behiry and Aly[20] improved intrusion detection in WSNs by integrating FS models, namely singular value decomposition

(SVD) and PCA, with K-means clustering improved by information gain (KMC-IG) technique for feature extraction and the synthetic minority oversampling technique (SMOTE) for data balancing. A DL-based feed-forward neural network (FNN) model was then employed to classify network traffic and detect cyberattacks accurately. Farid and Khalil[21] improved intrusion detection in wireless sensor networks (WSNs) by integrating advanced ML techniques, such as decision trees (DTs), RF, SVM, k-nearest neighbours (KNN) and ensemble methods with the SMOTE-Tomek technique to address class imbalance. The framework also employs sequential backwards selection (SBS) for optimal FS and robust data pre-processing to improve detection accuracy and reduce false positives. AboulEla et al.[22] reviewed and analysed AI-based cybersecurity methodologies for internet of medical things (IoMT) networks, focusing on ML, DL, hybrid ML-DL, transformer-based techniques and emerging approaches like graph-based and blockchain methods. Luthfi et al.[23] presented a method to improve software defect prediction by integrating advanced pre-processing techniques, such as Z-score standardisation and robust scaling, with the adaptive synthetic sampling (ADASYN) method for class imbalance. FS is optimised using the binary Harris Hawk Optimisation (BHHO) model, evaluated by kNN, and incorporated with ensemble learning (EL) models, such as RF, SVM and stacking, to improve classification performance. Al-Amiedy, Anbar and Belaton[24] detected selective forwarding (SF) attacks in low-power and lossy networks (LLNs) by integrating optimised data balancing using SMOTE, FS through binary particle swarm optimisation (BPSO) and attack detection with an optimised RF classifier tuned via GridSearchCV. Thamer Francis, Souri and İnanç[25] proposed an effective IDS for IIoT networks by utilising the split-point algorithm with attribute-reduced classifier (SPAARC) DT integrated with the firefly algorithm (FA) for FS. The proposed system utilises a software-defined networking (SDN) architecture to enhance centralised control and improve detection accuracy across IIoT environments.

Kocyigit et al.[26] presented a model to support phishing attack detection by employing a genetic algorithm (GA)-based FS method, integrated with local optimisation, to identify the most relevant URL features. This approach aims to enhance the performance of ML models by mitigating overfitting, computational cost and training time while maintaining high detection accuracy. Qiao et al.[27] developed a simple and efficient incentive mechanism for federated learning (FL) model in vehicular networks, thus improving clustering accuracy and mitigating network overhead and convergence time. Alfatemi et al.[28] improved DDoS attack detection by integrating diverse DNN models using combinatorial fusion analysis (CFA) to improve detection accuracy and robustness. Lv et al.[29] investigated a new front-end web attack by utilizing cloud object storage service vulnerabilities to bypass Content Security Policy (CSP), analyze its impact on real-world websites to eliminate the threat. Al-Shukaili, Kiah, and Ahmedy[30] improved detection of low-rate Distributed Denial of Service (LDDoS) attacks, specifically slowloris and slowhttptest, by optimizing feature selection using synthetic minority oversampling technique (SMOTE), recursive feature elimination, and DL models. Lu et al.[31] proposed AutoD, an unpacking system using Java Native Interface (JNI) layer deception-calls in Android Runtime (ART) for restoring decrypted Dex files in reinforced blockchain-wallet applications for detecting hidden malicious code. Pradeesh, Jeyakarthic, and Thirumalairaj[32] presented a sensor-enhanced hybrid framework using Adaptive Ensemble of Modular Classifiers (AEMC) and One-vs-Rest (OvR) classifiers for real-time multi-class detection and classification of DDoS attacks in SDNs. Lu et al.[33] presented DeepAutoD, a generic unpacking framework by utilizing deep deception call chains to restore original Dex files from reinforced Android apps, enabling accurate malicious code detection in distributed ML systems. Dilshad, Syed, and Rehman[34] improved DDoS attack detection in Internet of Vehicles (IoV) systems by employing the Gini index for feature selection and FL for decentralized, privacy-preserving model training. Gu et al.[35] proposed an interactive gradient shielding (IGS) and adaptive gradient shielding (AGS) methods to generate effective adversarial examples. Asuai et al.[36] developed an effective DDoS attack detection framework by utilizing a hybrid approach that combines the Three Conditions for Feature Aggregation (3ConFA) for robust feature selection and a 1D-CNN for deep temporal-spatial pattern learning. This integration seeks to improve detection accuracy while addressing class imbalance with the Adaptive Synthetic Sampling Approach (ADASYN). Table 1 summarises previous works on DDoS attacks.

Despite crucial improvements in DDoS detection and mitigation, various limitations still exist. Various models face difficulty due to high computational complexity and increased communication overhead, restricting their scalability in distributed and resource-constrained environments like IoV and SDN. Few techniques encounter difficulty in balancing dimensionality reduction with maintaining critical data, affecting detection accuracy. Moreover, class imbalance issues still exist, despite oversampling methods like SMOTE and ADASYN. Various models highlight the need for decentralized models such as FL, and while hybrid and ensemble models enhance detection, their interpretability and real-time applicability require additional enhancement. This research gap calls for efficient, scalable, privacy-preserving frameworks with robust feature selection and balanced datasets, aiming to optimize detection accuracy while minimizing resource consumption.

Research design and methodology

In this study, the RAIHFAD-RFE model was proposed for cybersecurity systems. The study aimed to analyse and propose efficient cybersecurity strategies for detecting, mitigating and preventing DDoS attacks using advanced techniques. The model comprises data pre-processing, feature selection, attack classification and parameter tuning. Figure 2 illustrates the workflow of the RAIHFAD-RFE method.

Pre-processing using Z-score

As a primary step, the RAIHFAD-RFE technique utilises the Z-score standardisation method for the data pre-processing stage to clean, transform and organise raw data into a structured format[37]. This technique was chosen for its efficiency in normalising features by centring data around a mean of zero and a standard deviation of one. It is specifically beneficial when features have varying scales; it ensures that each feature contributes equally

Authors	Years	Objectives	Techniques	Dataset	Performance Validation
Alrumaih and Alenazi[11]	2025	A new resilience structure is advanced to protect industrial controller networks against accessibility threats posed by DDoS attacks.	Industrial Control Systems	Own Dataset	Around 88% of normal throughput at 25% channel usage
Hu and Shi[12]	2025	Design communication and controller tactics are proven and can guarantee the coordination of CDNs with MCDSAs.	Lyapunov Stability Approach	-	-
Wang et al[13].	2025	To provide a reliable solution for higher-dimensionality data handling and DDoS attack recognition inside SDN, and deal with the immediate problems in these fields.	ARSAE-QGRU, SAE	CICDDoS-2019 and CIC-IDS-2017 Datasets	Accuracy rates of 97.2% and 97.9%
Balamurugan et al[14].	2024	The goal of this project is to identify potential solutions to this problem, including methods for preventing and mitigating these attacks.	NADP, NADP	Simulated Network Data	Effective Detection, Improved Mitigation
Hnamte et al[15].	2024	To present an innovative DDoS detection model within the SDN framework, this approach also provides insight into helpful findings and challenges related to utilising DNNs in real-time SDN environments.	DNN	In SDN, CIC-IDS-2018, and Kaggle DDoS Dataset	Accuracy rates of 99.98%, 100%, and 99.99%
Martinez et al[16].	2024	To introduce the Dual-space loss function and the Dual-space Prototypical Network, advancements engineered to detect DDoS attacks.	MLP with AMs	CIC-IDS Dataset	Accuracy of 94.85% and F1-Score of 94.71%
Ahmed et al[17].	2023	To recommend an ML-allowed trust-based routing protocol that determines the attacked nodes responsible for DDoS and packet suppression attacks.	ANN, SVM	DDoS Attack Dataset	-
Hossain and Islam[18]	2023	To introduce a novel ML-driven approach designed to fortify network security by effectively identifying botnet-based DDoS attacks.	RF, PCA, MI, SMOTE	Comprehensive SDN Traffic Data	High Accuracy, Balanced Accuracy
Emirmahmutoğlu and Atay[19]	2025	To improve anomaly-based IDS performance using heuristic FS and ML models.	PSO, FPA, DE	KDDCup99, NSL-KDD, UNSW-NB15, CSE-CIC-IDS2018	High Accuracy (~ 99% F1-Score)
Behiry and Aly[20]	2024	To improve WSN security for intrusion detection.	SVD, PCA, KMC-IG, SMOTE, FNN	NSL-KDD, UNSW-NB15, CICIDS2017	High Accuracy and Reliability
Farid and Khalil[21]	2025	To develop a balanced and accurate IDS system.	SMOTE-Tomek Balancing, SBS, Feature Standardisation, DT, RF, SVM, KNN	WSN-DS, UNSW-NB15	100% and 97.3% accuracy, < 1.2% false positives
AboulEla et al[22].	2024	To review and analyse AI-based cybersecurity techniques for intrusion detection in IoMT.	ML, DL, Hybrid ML-DL, Transformer-based Models, Graph and Blockchain Methods	IoT and IoMT Benchmark Datasets	Comprehensive evaluation, varied accuracy
Luthfi et al[23].	2025	To develop a robust classification framework.	Z-Score Standardisation, Robust Scaling, ADASYN, BHHO, kNN, RF, SVM, stacking	NASA MDP (MC1)	Accuracy 0.998, AUC 1.000
Al-Amiedy, Anbar, and Belaton[24]	2024	To develop an optimised approach for detecting SF attacks.	Data Preparation, SMOTE, BPSO, RF with GridSearchCV	Grid-based LLN Dataset	Accuracy 99.82%
Thamer Francis, Souri, and İnanç[25]	2025	To develop a high-accuracy IDS for IIoT networks.	SPAARC DT, FA, SDN-based Four-Layer Architecture	DDoS_SDN, XIIoT_ID	Accuracy ~ 99.99%, Near-Zero Error
Kocyigit et al[26].	2024	To enhance phishing attack detection.	GA, Locally Optimised Search, URL-based Phishing Detection	URL Phishing Dataset	Improved accuracy and efficiency
Qiao et al[27].	2023	To design a simple, efficient incentive mechanism for FL in vehicular networks.	Incentive Mechanism Design, High-Quality Agent Selection	Synthetic and Real-World Datasets	+ 2% Accuracy, 70% Overhead Reduction, 9% Faster Convergence
Alfatemi et al[28].	2025	To develop a model for improved DDoS attack identification.	Diverse DNN, CFA	Real Network Data	Higher Precision, Robust Detection
Lv et al[29].	2023	To investigate and mitigate a novel front-end web attack.	CSP	Data from Google and Amazon Object Storage Services	Security Breach Analysis
Al-Shukaili, Kiah, and Ahmedy[30]	2025	To improve the detection of two common LDDoS attack types.	LDDoS, SMOTE	cic-ids2017 Dataset	Accuracy Of 99.77%, Precision Of 95.27%, Recall of 95.63%, F1-Score of 95.45%, and AUC of 97.76%
Lu et al[31].	2020	To develop AutoD, an unpacking system for detecting hidden malicious code in reinforced blockchain wallet applications.	JNI, ART	Reinforced Blockchain Applications	Full Protection Repair
Pradeesh, Jeyakarthic, and Thirumalairaj[32]	2025	To identify specific attack vectors while adapting to growing threats.	AEMC, OvR	Real-World and Simulated Data	High Precision, Recall
Lu et al[33].	2021	To develop DeepAutoD, a generic unpacking framework that reveals hidden malicious code.	DeepAutoD, Reinforcement Elimination, Adaptable to Android Versions	Mainstream Android Apps	Superior Safety, Effectiveness
Dilshad, Syed, and Rehman[34]	2025	To improve DDoS attack detection in IoV.	Gini Index Feature Selection, FL	IoV Network Traffic Data	91% Accuracy, Varied Precision
Continued					

Authors	Years	Objectives	Techniques	Dataset	Performance Validation
Gu et al[35].	2020	To understand and improve adversarial attacks on DNNs.	DNN, IGS, AGS	Image Classification Datasets	Competition Winner, High Effectiveness
Asuai et al[36].	2025	To develop an accurate hybrid DL model for detecting DDoS attacks.	3ConFA, 1D-CNN, ADASYN, RFECV, Softmax Layer	Raw Network Traffic Data (Imbalanced, Balanced by ADASYN)	99.42% Training Accuracy, 99.35% F1-Score, 99.87% AUC-ROC; Test Accuracy 99.56%, Precision 99.61%, F1-Score 99.50%, AUC-ROC 0.9982

Table 1. Comparison of existing studies on DDoS attacks using ML and DL models.

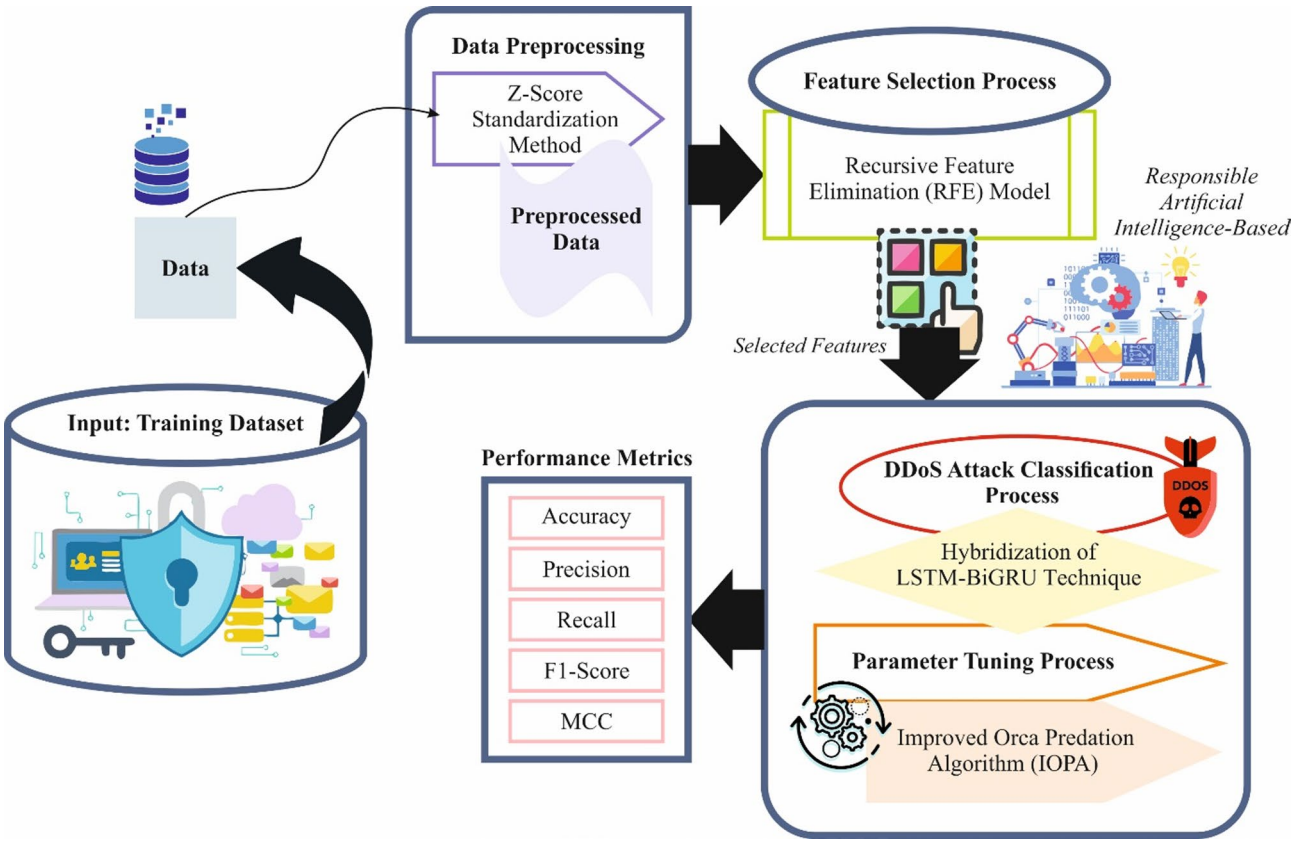

Fig. 2. Work flow process of the RAIHFAD-RFE model.

to the learning process. The model is less sensitive to outliers, making it more robust for real-world network traffic data and is efficient in convergence speed and stability of gradient-based optimisation methods used in DL techniques, such as long short-term memory (LSTM) and bidirectional gated recurrent unit (BiGRU). This standardisation technique also helps prevent the model from being biased towards features with larger numerical ranges. Moreover, Z-score normalisation is widely applicable and consistent across datasets, thus enhancing generalisation.

The proposed model adjusts the features by subtracting the mean and then dividing them by the standard deviation, resulting in a standard deviation of 1 and a mean of 0. It is effective for models that typically assume distributed input features, such as logistic and linear regression. The z-score normalisation for feature x' is computed utilising the following equation:

$$x' = \frac{x - mean\,(x)}{std\,(x)} \tag{1}$$

Here, x' depicts the normalised value, x indicates the original value, $std\,(x)$ refers to the standard deviation of x and mean (x) denotes the average feature x. The other normalisation models include the interquartile range (IQR), which depicts the extent of statistical dispersion, denoting how spread out the data is. IQR is measured by the difference between the 75th and 25th percentiles. The quartiles are described as Q1 (lower quartile),

Q2 (median), and Q3 (upper quartile); here, Q1 and Q3 are equivalent to the 25th and 75th percentiles. The following equation specifies the IQR:

$$IQR = Q3 - Q1 \tag{2}$$

Selecting a proper normalisation model plays an essential role in enhancing the performance of the LSTM-BiGRU method. Normalising input variables to a common scale might enhance the efficacy of learning models and improve the accuracy of predictions. Since a diverse normalisation model manages data scales and outliers, the selection of models can significantly influence how effectively the techniques acquire patterns in data. Determining the most appropriate methodology can necessitate empirical assessment or insights from preceding analysis utilising comparable datasets and DL frameworks.

Dimensionality reduction procedure

The RFE model is employed for the FS process to recognise and preserve the most significant features for increasing the model's performance[38]. This model was chosen for its capability in systematically selecting the most relevant features by recursively removing the least significant ones based on model performance. This method relies solely on statistical measures and considers feature importance within the learning algorithm, resulting in a more informed selection. It effectually mitigates dimensionality, which decreases overfitting and improves computational efficiency. Compared to embedded methods, RFE presents greater flexibility in pairing with diverse models. Its iterative nature ensures that optimal feature subsets are detected for improved model accuracy. RFE is particularly suitable for complex tasks, such as DDoS detection, where eliminating irrelevant features significantly enhances performance.

RFE is one of the FS approaches employed for recognising the essential features in a dataset by iteratively extracting less related aspects, depending on their performance. In this study, the datasets comprised higher-dimensional data, and RFE is specifically beneficial for reducing redundancy and enhancing the efficacy of ML techniques. To select only the most crucial features, RFE reduces computational overhead, creating methodologies that are more interpretable and faster, enhances precision and handles higher dimensions. Intrusion detection datasets frequently have a great number of attributes. RFE guarantees that only effectual aspects are retained. RFE is employed to pre-process and scale datasets for selecting the most substantial elements before training ML methodologies, such as RF, decision tree and logistic regression.

A base estimator was employed to assess significant features using an underlying technique. For instance, RF offers the significance of feature scores, depending on its DT. Primarily, the methodology is trained on the entire set of features. Assume that X is the input feature matrix, y indicates targeted labels, and M signifies the ML technique employed in RFE. The significance of feature scores for the ith feature is specified as follows:

$$I_i = Importance\ of\ feature\ x_i\ as\ determined\ by\ M \tag{3}$$

The least significant features were eliminated iteratively. This procedure repeats until the chosen feature count k is designated. Let $X^{(T)}$ depict the feature matrix at iteration t. At all iterations, training M on $X^{(T)}$ to calculate significant scores. Eliminate r features with the least significant scores:

$$X^{(t+1)} = X^{(t)} \setminus \{x_1,\ x_2, \ldots, x_n\} \tag{4}$$

Now $\{x_1,\ x_2,\ \ldots\ , x_n\}$ refers to less significant features. The procedure halts after the recollected feature counts achieve the preferred number k, halt

$$if\ \left|X^{(\tau+1)}\right| = k \tag{5}$$

The chosen features are employed for training the final model M_{final}:

$$M_{final} = Train\left(M,\ X^{(T)},\ y\right) \tag{6}$$

Once features are selected using RFE, datasets with reduced features are employed to train intrusion detection techniques, enhancing their computational efficacy and prediction accuracy. RF and DT classifiers were employed as the base techniques for RFE to effectively use their ability.

Initialisation:

Selected Features = {X_1, X_2, ……., X_n}

RFE Loop:

For I = n to k (in reverse order)

Train Model:

$Model_i$ = Model ($SelectedFeatures_i$)

Update Model: $Model_{i-1}$= Model ($SelectedFeatures_{i-1}$)

Final Model:

$FinalModel = Model_k$

Algorithm 1: Pseudocode of RFE

Hybridisation of DDoS attack classification

For the DDoS attack classification procedure, the RAIHFAD-RFE model implements hybridisation of the LSTM-BiGRU technique[39]. This hybrid model was chosen to employ the merits of both architectures in handling sequential network traffic data. LSTM outperforms at capturing long-term dependencies, while BiGRU processes data in both forward and backward directions for better context understanding. The capability of the model is improved by this integrated model for detecting complex and evolving attack patterns compared to standalone RNNs or CNNs. Unlike conventional ML models, hybrid DL models adapt better to temporal dynamics. It also enhances accuracy, robustness, and generalisation in imbalanced or noisy datasets. Overall, the hybrid model provides a more reliable and efficient solution for DDoS detection. Figure 3 specifies the framework of the LSTM-BiGRU model.

Generally, LSTM networks are efficient in predicting and modelling time-series data by presenting output, input, and forget gates. These gates help alleviate the gradient vanishing problems and gradient explosion to some extent. The forget gate, signified by f_t, controls whether the data must be forgotten. The input gate controls which novel information is added to the memory cell. The output gate, denoted as O_t, limits the output of the hidden layer (HL) vector. The reliable equations are presented in Eq. (7) to (12).

$$f_t = \sigma\ (W_f\,[h_{t-1},\ x_t] + b_f) \tag{7}$$

$$i_t = \sigma\ (W_i\,[h_{t-1}, x_t] + b_i) \tag{8}$$

$$o_t = \sigma\ (W_o\,[h_{t-1}, x_t] + b_o) \tag{9}$$

$$\widetilde{C}_t = \tanh\,(W_c\,[h_{t-1}, x_t] + b_c) \tag{10}$$

$$C_t = f_c \odot\ C_{t-1} + i_t\widetilde{C}_t \tag{11}$$

$$h_t = O_t \odot\ \tanh\,(C_t) \tag{12}$$

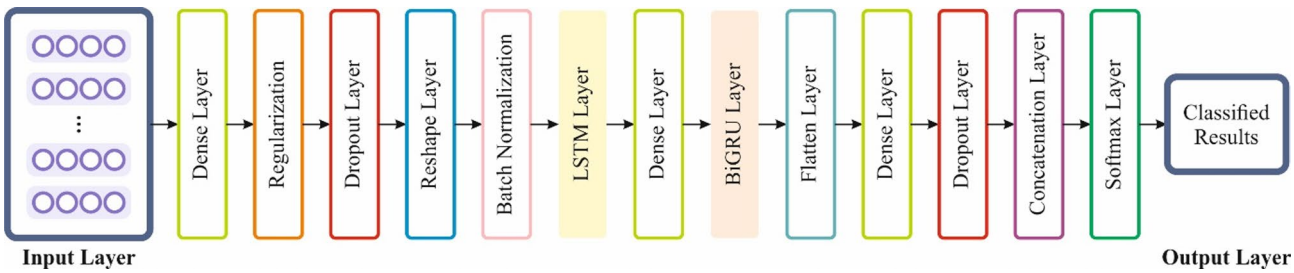

Fig. 3. Structure of the LSTM-BiGRU technique.

Whereas: x_t denotes input at time step t; h_t refers to HL at time step t; $\widetilde{C}_t$ represents candidate cell state at time step t; C_t signifies upgraded cell state at time step t; W_f, W_i, W_o, and W_c designate the weighted matrices equivalent to every module; b_f, b_i, b_o, and b_c represents bias matrices akin to every module; σ characterises the activation function of the Sigmoid; and $\odot$ means Hadamard product.

Additionally, BiGRU is a neural network that incorporates a bidirectional GRU and RNN. Compared to conventional GRUs, RNNs better address the issues of explosion and gradient vanishing while capturing longer-term dependencies in sequences. The bidirectional RNN also increases the method by handling either past or future inputs, allowing improved sequence data processing. BiGRU handles data sequences by initially passing the input sequence through dual GRU networks, one in the forward direction and the other in the backward direction. The outputs from either direction are then connected to make the final output. Additionally, BiGRU is primarily beneficial in capturing dependencies within sequences, as it can consider either previous or future information. Therefore, adopting the BiGRU method to address the related intrusion of these features will enhance prediction precision by reducing the model's error. The essential elements of a GRU consist of updates and reset gates that control the upgrading and use of the HL over nonlinear transformations. The consistent equations are presented in Eqs. (13) to (16).

$$r_t = \sigma\ (W_r x_t + U_r h_{t-1} + b_r) \tag{13}$$

$$z_t = \sigma\ (W_Z x_t + U_z h_{t-1} + b_Z) \tag{14}$$

$$h_t^* = \tanh\left(W_h x_t + r_t U_r h_{t-1} + b_h\right) \tag{15}$$

$$h_t = (1 - z_t)\, h_t^* + z_t h_{t-1} \tag{16}$$

Here, r_t and z_t denote reset and update gates; $\tanh$ represents the activation function of the hyperbolic tangent; h_t^* signifies candidate HL at the time step ; W_r, W_Z, and W_h symbolise the weighted matrices for all modules; and b_r, b_Z, and b_h illustrate bias matrices for all modules.

IOPA-based hyperparameter tuning model

To further optimise model performance, the IOPA is utilised for hyperparameter tuning to ensure that the best hyperparameters are chosen for enhanced accuracy[40]. This model was selected for its superior balance between exploration and exploitation, which assists in avoiding local optima more effectively than conventional methods, such as grid search or GAs. The model performs efficient searching of the hyperparameter space, resulting in faster convergence and improved optimisation. Compared to other metaheuristic algorithms, it requires fewer iterations to achieve better performance, making it a computationally efficient approach. This results in improved model accuracy and robustness, especially crucial for complex architectures like the hybrid LSTM-BiGRU used in DDoS attack detection. Overall, IOPA presents a powerful and efficient approach for fine-tuning model parameters in dynamic network environments.

The orca predator algorithm (OPA) replicates the foraging behaviour of orcas (killer whales). The foraging tactic of the individual consists of three phases: attacking, driving, and surrounding prey. The presented model has improved the parameters for surroundings and drives for striking a balance between exploitation and exploration. During the attack phase, the best solution is recognised without offering the particle categories in consideration of numerous optimal orcas (candidates) in addition to those designated randomly. The presented OPA model is numerically described as follows:

1. The initial step is to assemble a group of orcas. The model recommends using N_n individuals, all of whom are located in different dimensional areas. This process is verified by the succeeding Eq. (17):

$$X = [x1,\ x2,\ x3,\ \ldots,\ xN_n] = \begin{bmatrix} X_{1,1} & X_{1,2} & \cdots & X_{1,Dim} \\ X_{2,1} & X_{2,2} & \cdots & X_{2,Dim} \\ \vdots & \vdots & \vdots & \vdots \\ X_{N_n,1} & X_{N_n,2} & \cdots & X_{N_n,Dim} \end{bmatrix} \tag{17}$$

Whereas, the population candidate solution is represented by X. xN_n establishes the N^{th} candidate location. Dim has portrayed the population size.

2. 2. The second step is the chasing stage, which has two sub-steps: driving and encircling. The variable p_1 is used to improve the probability of individuals following these dual stages. Two conditions determine the choice between using the encircling or driving process. When the random number is improved, the driving process should be used for p1. Alternatively, the encircling process should be applied.
3. 3. The third step is the driving procedure, which is crucial for ensuring that group members maintain their primary position and remain close to the prey. The objective is to prevent individuals from travelling apart from their goals.

$$V_{chase,1,i}^t = a \times \left(d \times x_{best}^t - F \times \left(b \times M^t + c \times x_i^t\right)\right) \tag{18}$$

$$V_{chase,2,i}^t = e \times x_{best}^t - x_i^t \tag{19}$$

Whereas, the iterations' numbers are represented by t. $V_{chase,1,\,i}^t$ and $V_{chase,2,}$ specify the chasing speed following the choice of the first and second stages. The random amounts consist of d and b, which are in the

interval of $(0,1)$, and e signifies stochastic numbers that are in the range (0,2). For chasing tactic selection, q is applied that varies among $(0,1)$, and the F value equivalents two. M represents the orca population's mean position.

$$M = \frac{\sum_{i=1}^{N_n} x_i^t}{N_n} \tag{20}$$

$$c = 1 - b \tag{21}$$

In this context, there are two different methods for chasing that depend significantly on the population size. The 1 st model is applied if $rand > q$, and the 2nd model is applied if $rand \leq q$.

$$\begin{cases} x_{chase,1,i}^t = x_i^t + V_{chase,1,i}^t \;\; if\, rand > q \\ x_{chase,2,i}^t = x_i^t + V_{chase,2,i}^t \;\; if\, rand \leq q \end{cases} \tag{22}$$

4. The fourth step is to surround the prey. Here, the development of candidates utilising three arbitrary individuals is defined in Eqs. (23) and (24):

$$x_{chase,3,i,k}^t = x_{d1,k}^t + u \times \left(x_{d2,k}^t - x_{d3,k}^t\right) \tag{23}$$

$$u = 2 \times \left(randn - \frac{1}{2}\right) \times \frac{\mathrm{Max}_{itr} - t}{\mathrm{Max}_{itr}} \tag{24}$$

Now, the variable Max_{itr} exemplifies the maximal number of iterations. Candidates chosen at random are represented by 1, $d2$, and $d3$, and they are not equal. If the third chasing tactic is selected, the state is specified by $x_{cha\,se,3,i,k}^t$..

5. The fifth step is to develop the surroundings of the victim, where every individual's state has improved.

$$\begin{cases} x_{chase,i}^t = x_{chase,i}^t & if\, f\left(x_{chase,i}^t\right) < f\left(x_i^t\right) \\ x_{chase,i}^t = x_i^t & if\, f\left(x_{chase,i}^t\right) \geq f\left(x_i^t\right) \end{cases} \tag{25}$$

Whereas the cost function is associated with $x_{chase,\,i}^t$ was portrayed by $f\left(x_{chase,\,i}^t\right)$, and the function of cost, which is associated with x_i^t was established by $f\left(x_i^t\right)$.

6. The sixth step is to attack on the prey. The best four individuals are positioned in the top-four places. The candidates' locations and their speed of movement during the attack are verified utilising the equations below:

$$V_{\alpha\, ttack,1,i}^t = \frac{(x_1^t + x_2^t + x_3^t + x_4^t)}{4} - x_{chase,i}^t \tag{26}$$

$$V_{\alpha\, ttack,2,i}^t = \frac{\left(x_{chase,d1}^t + x_{chase,d2}^t + x_{chase,d3}^t\right)}{3} - x_i^t \tag{27}$$

$$x_{attack,i}^t = x_{chase,i}^t + g_1 \times V_{attack,1,i}^t + g_2 \times V_{attack,2,i}^t \tag{28}$$

Next, the vector speed is proven by $V_{attack\,2}$ and V_{attack} 1. The best individuals in the optimal positions are identified by x_1^t, x_2^t, x_3^t, and x_4^t. The three randomly chosen individuals are demonstrated by 1, $d2$, and $d3$ to differ from each other. The state designated following the attacking stage is described by $x_{attack,i}^t$. The variables g_1 and g_2 specify a random value within the interval of $(0, 2)$ and -2.5 to 2.5.

7. The seventh step is the attack stage. The orcas' positions were verified by the lower boundary (lb) problems.

As previously stated, the primary objective of this paper is to utilise OPA for optimal parameter selection. Selecting the best parameters is a complex task that involves numerous steps for the typical OPA to achieve accurate results and convergence rates in complex states. To address these difficulties, enhancements are made to increase the efficacy and robustness of the method, resulting in improvements in the IOPA. The establishment of the IOPA is the insertion of the removal stage. At the start of every iteration, the model tactically removes ineffective individuals to create space for unique individuals within the novel solution area. This new model significantly enhances the model's ability to perform an exploration, enabling it to examine numerous pathways towards the optimal solution.

Eliminating the caught individuals in local ideals helps the model avoid suboptimal solutions and improves exploration in better ways. The characteristics of the IOPA technique are a dynamic area of exploration, frequently adding novel initial points. The adaptive feature enables the model to avoid getting caught in suboptimal solutions and expands its solution area. Removing the minimum efficient starting point's assurances that computational sources are correctly concentrated on the more predictable regions within the solution area. The removal stage is an appropriate filter method that leads the model towards efficient solution spaces for exploration.

The projected developments offer various advantages, including improved precision and enhanced exploration capabilities. The IOPA examines different solutions by dynamically improving the solution area and giving new early points that reduce the probability of getting caught in local ideals. This model's improved approach to its search method and exploration of dissimilar paths differentiates it from the standard OPA, making it particularly suitable for composite parameter identification challenges. Table 2 illustrates the comparative analysis of IOPA

Criterion	IOPA	BO	CMA-ES	PSO	GA	Performance
Convergence Speed	Fast	Moderate	Moderate	Moderate	Moderate	The tuning is improved via iterative removal.
Swarm Diversity	High (removes stagnated agents)	Moderate	Moderate	Moderate	Moderate	Exploration is maintained better than others.
Local Minima Avoidance	Effective	Prone to local minima	Moderate	Moderate	Moderate	Local traps are evaded by iterative removal.
Computational Overhead	Moderate (1.2–1.5× runtime)	Low	Low to Moderate	Less Effective	Less Effective	Slightly improved runtime is justified by gains.
Accuracy Improvement	3–5% higher	Good	Comparable	Moderate	Moderate	Better accuracy offsets overhead.

Table 2. Comparison study of IOPA with advanced optimizers.

CIC-IDS-2017 Dataset			
S.no	**Type**	**Traffic Type**	**Count**
1	**Attacks**	TFP-Parator	2500
2		SSH-Parator	2500
3		DoS Slowlorls	2500
4		DoS Slowhttptest	2500
5		DoS Hulk	2500
6		DoS GolderEye	2500
7		Web Attack-BF	1500
8		Bot	1500
9		DDoS	2500
10		Port Scan	2500
11	**Benign**	Normal	2500
Total Number of Count			**25,500**

Table 3. Details of the CIC-IDS-2017 dataset.

and advanced optimizers for hyperparameter tuning in DDoS detection. The key differences between IOPA and other optimizers such as Bayesian Optimization (BO) and covariance matrix adaptation evolution strategy (CMA-ES), particle swarm optimization (PSO), and genetic algorithm (GA) for DDoS tuning. It also highlights the faster convergence and better avoidance of local minima due to its iterative removal step, which slightly enhances computational overhead. This trade-off results in an enhanced accuracy, demonstrating the efficiency of the IOPA model for DDoS detection tasks.

The IOPA technique creates a fitness function (FF) to achieve greater performance in classification. It defines an affirmative number to characterise the boosted outcome of the candidate solutions. The minimisation of the classification error rate was deliberated as the FF, as given in Eq. (29).

$$\begin{aligned} fitness\,(x_i) &= Classifier\ Error\ Rate\,(x_i) \\ &= \frac{number\ of\ misclassified\ samples}{Total\ no\ of\ samples} \times\ 100 \end{aligned} \tag{29}$$

Results analysis and discussion

The performance simulation of the RAIHFAD-RFE model was evaluated using two datasets: CIC-IDS-2017[41] and Edge-IIoT[42]. The CIC-IDS-2017 dataset comprises a total of 25,500 counts across 11 classes. Table 3 portrays the complete details of the CIC-IDS-2017 dataset. The complete number of attributes was 78, but only 32 attributes were selected.

Figure 4 depicts the classifier results of the RAIHFAD-RFE technique on the CIC-IDS-2017 dataset. Figure 4a and c show the confusion matrices, demonstrating the accurate detection and classification of all classes on a 70:30 split. Figure 4b illustrates the PR examination, demonstrating the top performance for each class. Ultimately, Fig. 4d illustrates the ROC investigation, showing capable outcomes with higher ROC values to separate the classes.

Table 4; Fig. 5 illustrate the DDoS attack detection capabilities of the RAIHFAD-RFE approach using the CIC-IDS-2017 dataset. With 70% TRPHE, the proposed RAIHFAD-RFE model attains an average $accu_y$ of 99.31%, $prec_n$ of 96.15%, $reca_l$ of 95.99%, $F1_{Score}$ of 96.06%, and MCC of 95.68%. Finally, under 30% TSPHE, the proposed RAIHFAD-RFE model attains an average $accu_y$ of 99.35%, $prec_n$ of 96.36%, $reca_l$ of 96.22%, $F1_{Score}$ of 96.28%, and MCC of 95.93%.

Figure 6 reveals the classifier results of the RAIHFAD-RFE methodology in the CIC-IDS-2017 dataset. Figure 6a illustrates the accuracy inspection of the RAIHFAD-RFE methodology. The figure indicates that the RAIHFAD-RFE methodology presents increasing values with increasing epoch counts. Additionally, the

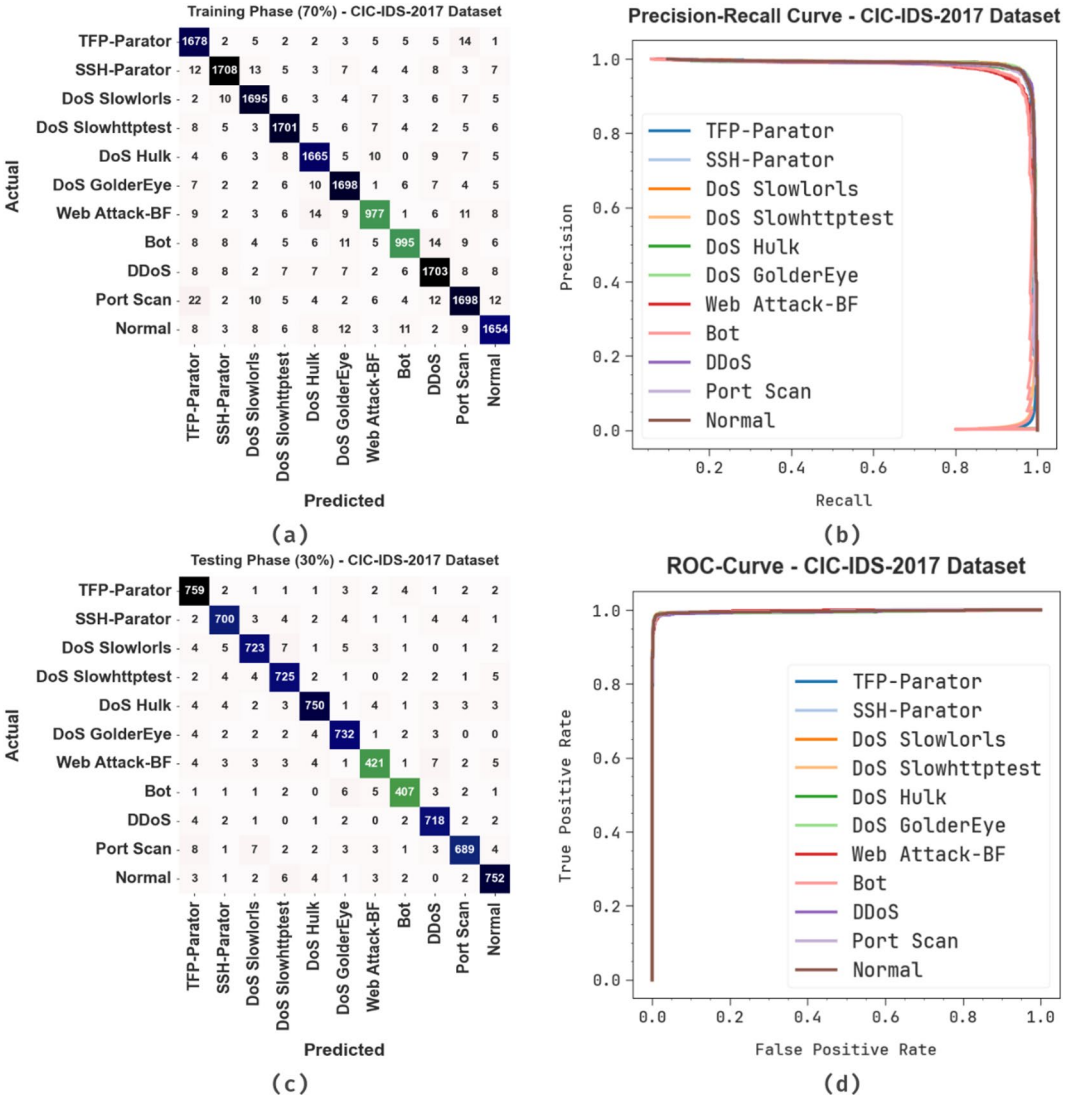

Fig. 4. CIC-IDS-2017 dataset: (a, c) 70% and 30% confusion matrices and (b, d) PR and ROC curves.

stable rise in validation over training demonstrates that the RAIHFAD-RFE technique efficiently learns from the test dataset. Figure 6b portrays the loss analysis of the RAIHFAD-RFE technique. The results specify that the RAIHFAD-RFE technique achieves close training and validation loss values. The RAIHFAD-RFE technique learns capably from the test dataset.

Table 5; Fig. 7 present a comparative analysis of the RAIHFAD-RFE technique on the CIC-IDS-2017 dataset, along with current methods, using various measures[43–45]. The table values indicate that the present methodologies, namely the KPCA-RN-SVM-LR, Naïve Bayes (NB), GRU-LSTM, PSO-LSTM, PRO-DLBIDCPS, BBFO-GRU and CO-Algorithm models, have shown the worst performance. However, the proposed RAIHFAD-RFE technique produced higher $accu_y$, $prec_n$, $reca_l$ and $F1_{Score}$ of 99.35%, 96.36%, 96.22% and 96.28%, respectively.

Table 6; Fig. 8 specify the ablation study of the RAIHFAD-RFE technique. The ablation study highlights the individual and combined impacts of key components in the RAIHFAD-RFE technique on the CIC-IDS 2017 dataset. Using only RFE, the model achieved an $accu_y$ of 97.50%, $prec_n$ of 94.41%, $reca_l$ of 94.08% and $F1_{Score}$ of 94.40%, illustrating the significance of effective FS. Incorporating IOPA for hyperparameter tuning improved performance to an $accu_y$ of 98.20%, $prec_n$ of 95.16%, $reca_l$ of 94.79% and $F1_{Score}$ of 95.03%. The LSTM-BiGRU classifier additionally enhanced results, reaching an $accu_y$ of 98.78%, $prec_n$ of 95.75%, $reca_l$ of 95.42% and $F1_{Score}$ of 95.62%. Finally, the RAIHFAD-RFE model integrating RFE, IOPA, and LSTM-BiGRU achieved the highest performance with an $accu_y$ of 99.35%, $prec_n$ of 96.36%, $reca_l$ of 96.22% and $F1_{Score}$ of 96.28%, demonstrating the efficiency of each module and their synergistic impact when combined.

The Edge-IIoT dataset comprises 48,000 records across 12 distinct event types. The details of the Edge-IIoT dataset are shown in Table 7. This dataset contains 63 features, but only 27 features were selected.

Figure 9 illustrates the classifier outcomes of the RAIHFAD-RFE technique on the Edge-IIoT dataset. Figure 9a and c illustrates the confusion matrix, showing the correct detection and classification of each class at

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC
TRPHE (70%)					
TFP-Parator	99.26	95.02	97.44	96.22	95.82
SSH-Parator	99.36	97.27	96.28	96.77	96.42
DoS Slowlorls	99.41	96.97	96.97	96.97	96.64
DoS Slowhttptest	99.40	96.81	97.09	96.95	96.62
DoS Hulk	99.33	96.41	96.69	96.55	96.18
DoS GolderEye	99.35	96.26	97.14	96.70	96.34
Web Attack-BF	99.33	95.13	93.40	94.26	93.91
Bot	99.33	95.77	92.90	94.31	93.97
DDoS	99.25	96.00	96.43	96.21	95.80
Port Scan	99.13	95.66	95.55	95.61	95.12
Normal	99.25	96.33	95.94	96.13	95.72
Average	**99.31**	**96.15**	**95.99**	**96.06**	**95.68**
THE (30%)					
TFP-Parator	99.28	95.47	97.56	96.50	96.11
SSH-Parator	99.33	96.55	96.42	96.49	96.12
DoS Slowlorls	99.28	96.53	96.14	96.34	95.94
DoS Slowhttptest	99.31	96.03	96.93	96.47	96.09
DoS Hulk	99.36	97.28	96.40	96.84	96.48
DoS GolderEye	99.39	96.44	97.34	96.89	96.55
Web Attack-BF	99.28	95.03	92.73	93.87	93.49
Bot	99.49	95.99	94.87	95.43	95.16
DDoS	99.45	96.51	97.82	97.16	96.86
Port Scan	99.31	97.32	95.30	96.30	95.92
Normal	99.36	96.78	96.91	96.84	96.49
Average	**99.35**	**96.36**	**96.22**	**96.28**	**95.93**

Table 4. DDoS attack detection of the RAIHFAD-RFE model on the CIC-IDS-2017 dataset.

a 70:30 ratio. Figure 9b clarifies the PR analysis, specifying the maximal outcomes across each class. Ultimately, Fig. 9d illuminates the ROC evaluation, establishing efficacious results with superior ROC values for individual classes.

Table 8; Fig. 10 describe the DDoS attack detection of the RAIHFAD-RFE technique at the Edge-IIoT dataset. Based on 70% TRPHE, the RAIHFAD-RFE technique achieved an average $accu_y$ of 99.39%, $prec_n$ of 96.37%, $reca_l$ of 96.37%, $F1_{Score}$ of 96.37% and MCC of 96.04%. Also, on 30% TSPHE, the RAIHFAD-RFE model attained an average $accu_y$ of 99.38%, $prec_n$ of 99.30%, $reca_l$ of 96.29%, $F1_{Score}$ of 96.29% and MCC of 95.96%.

Figure 11 depicts the classifier outcomes of the RAIHFAD-RFE method under the Edge-IIoT dataset. Figure 11a shows the accuracy examination of the RAIHFAD-RFE method. The figure suggests that the RAIHFAD-RFE method provides increasing values over successive epochs. In addition, the consistent progress in validation relative to training demonstrates that the RAIHFAD-RFE method effectively learns from the test dataset. Figure 11b reveals the loss analysis of the RAIHFAD-RFE method. The outcomes denote that the RAIHFAD-RFE method accomplishes similar training and validation loss values. It is highlighted that the RAIHFAD-RFE model learns effectively from the test dataset.

Table 9; Fig. 12 present a comparative analysis of the RAIHFAD-RFE approach on the Edge-IIoT dataset, along with existing techniques, using various metrics. The table values confirm that the current methods, such as the Shallow ANN, Isolated LSTM, CNN, RF, SVM, DNN and Inception Time techniques, illustrate the poorest performance. However, the RAIHFAD-RFE model achieved the highest $accu_y$, $prec_n$, $reca_l$, and $F1_{Score}$ of 99.39%, 96.37%, 96.37% and 96.37%, respectively.

Table 10; Fig. 13 show the ablation study analysis of the RAIHFAD-RFE approach. Using RFE alone resulted in an $accu_y$ of 97.38%, $prec_n$ of 94.71%, $reca_l$ of 94.30% and $F1_{Score}$ of 94.51%, indicating solid baseline performance from FS. When the IOPA was applied for hyperparameter tuning, the model achieved an $accu_y$ of 98.14%, $prec_n$ of 95.35%, $reca_l$ of 95.08% and $F1_{Score}$ of 95.16%, confirming its tuning effectiveness. The LSTM-BiGRU classifier exhibits further improvements, providing an $accu_y$ of 98.86%, $prec_n$ of 95.86%, $reca_l$ of 95.74% and $F1_{Score}$ of 95.83%, highlighting the power of temporal feature learning. The RAIHFAD-RFE model, which integrates RFE, IOPA and LSTM-BiGRU, delivered the highest performance with an $accu_y$ of 99.39%, $prec_n$ of 96.37%, $reca_l$ of 96.37% and $F1_{Score}$ of 96.37%, confirming the superiority of the model.

Conclusion

The study presented in this manuscript, proposed the RAIHFAD-RFE technique for cybersecurity systems. The RAIHFAD-RFE technique utilises the Z-score standardisation method for the data pre-processing stage to clean,

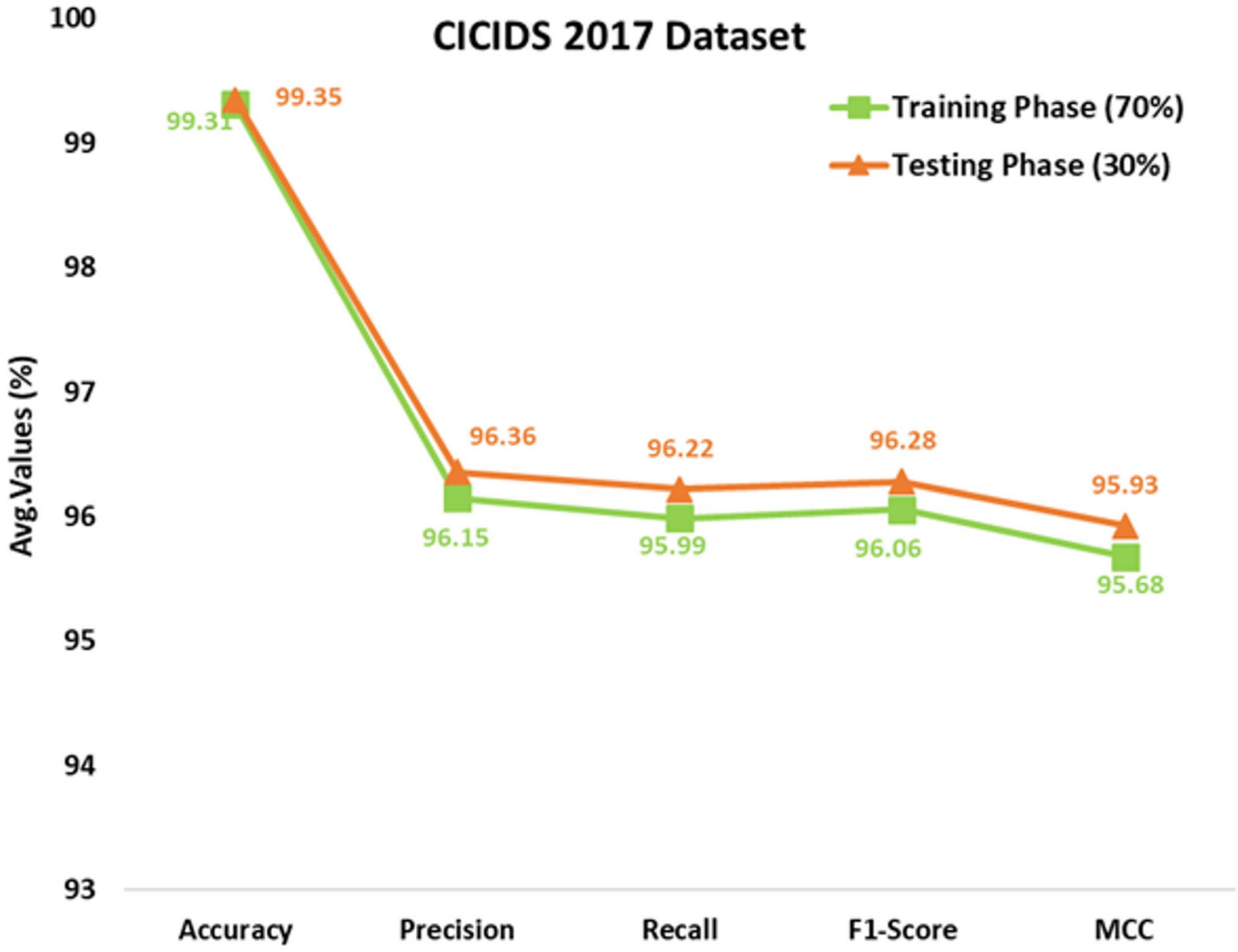

Fig. 5. Average values of the RAIHFAD-RFE model on the CIC-IDS-2017 dataset.

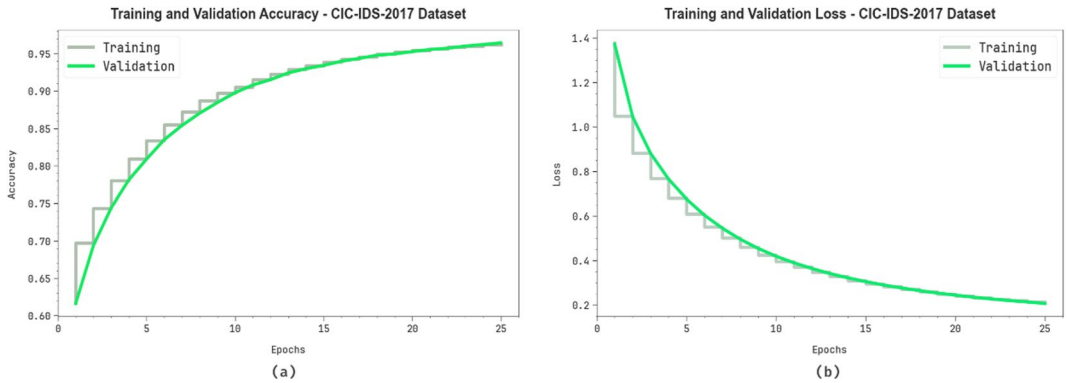

Fig. 6. (**a**) Accuracy and (**b**) loss curves on the CIC-IDS-2017 dataset.

transform and organise raw data into a structured format. Furthermore, the RFE model was employed for the FS process to recognise and maintain the most essential features for improving the model's performance. For the DDoS attack classification procedure, the RAIHFAD-RFE used hybridisation of the LSTM-BiGRU technique. To further optimises the model performance, the IOPA was utilised for hyperparameter tuning to ensure that the best hyperparameters are selected for enhanced accuracy. A comprehensive experimental analysis of the RAIHFAD-RFE model was performed under the CIC-IDS-2017 and Edge-IIoT datasets. The comparative analysis of the RAIHFAD-RFE approach provided superior accuracy values of 99.35% and 99.39%, respectively, compared to the existing models on the dual dataset.

CIC-IDS 2017 Dataset						
Approach	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	**Inference Latency (ms)**	**Memory Footprint (MB)**
KPCA-RN-SVM-LR	98.00	89.48	89.37	96.01	19.79	979
Naïve Bayes	88.96	93.36	90.89	95.69	19.64	962
GRU-LSTM	98.89	93.04	89.16	92.01	19.17	472
PSO-LSTM	94.69	93.77	95.99	93.57	19.34	674
PRO-DLBIDCPS	98.80	93.17	89.07	89.57	11.44	321
BBFO-GRU Model	98.10	95.81	95.86	96.07	16.54	766
CO-Algorithm	98.10	90.44	94.44	94.55	19.87	556
RAIHFAD-RFE	99.35	96.36	96.22	96.28	8.57	281

Table 5. Comparative analysis of the RAIHFAD-RFE method on the CIC-IDS-2017 dataset[43–45].

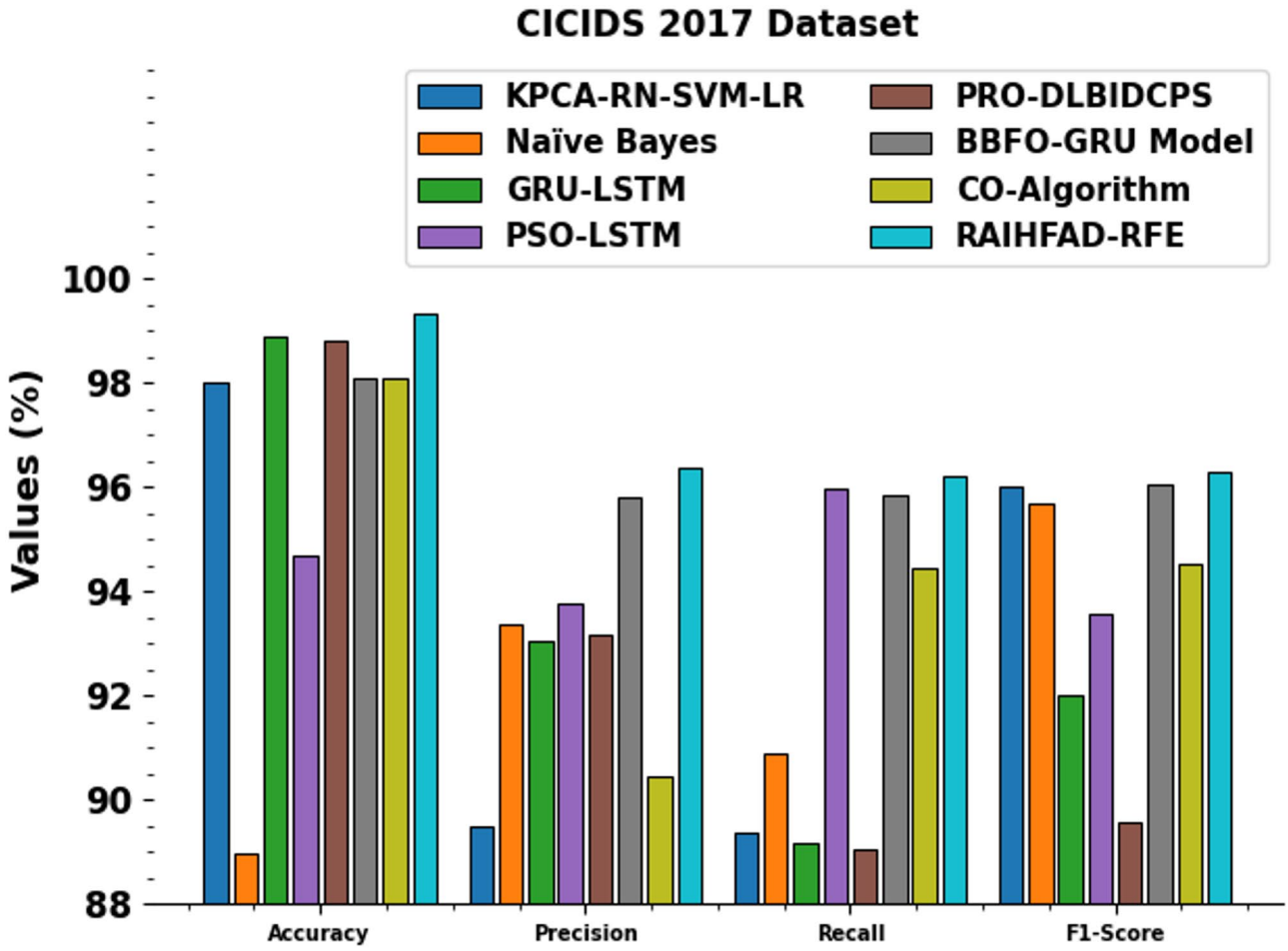

Fig. 7. Comparative analysis of the RAIHFAD-RFE method on the CIC-IDS-2017 dataset.

CIC-IDS 2017 Dataset				
Approach	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$
RFE	97.50	94.41	94.08	94.40
IOPA	98.20	95.16	94.79	95.03
LSTM-BiGRU	98.78	95.75	95.42	95.62
RAIHFAD-RFE	99.35	96.36	96.22	96.28

Table 6. Ablation study results comparing the RAIHFAD-RFE method on the CIC-IDS-2017 dataset.

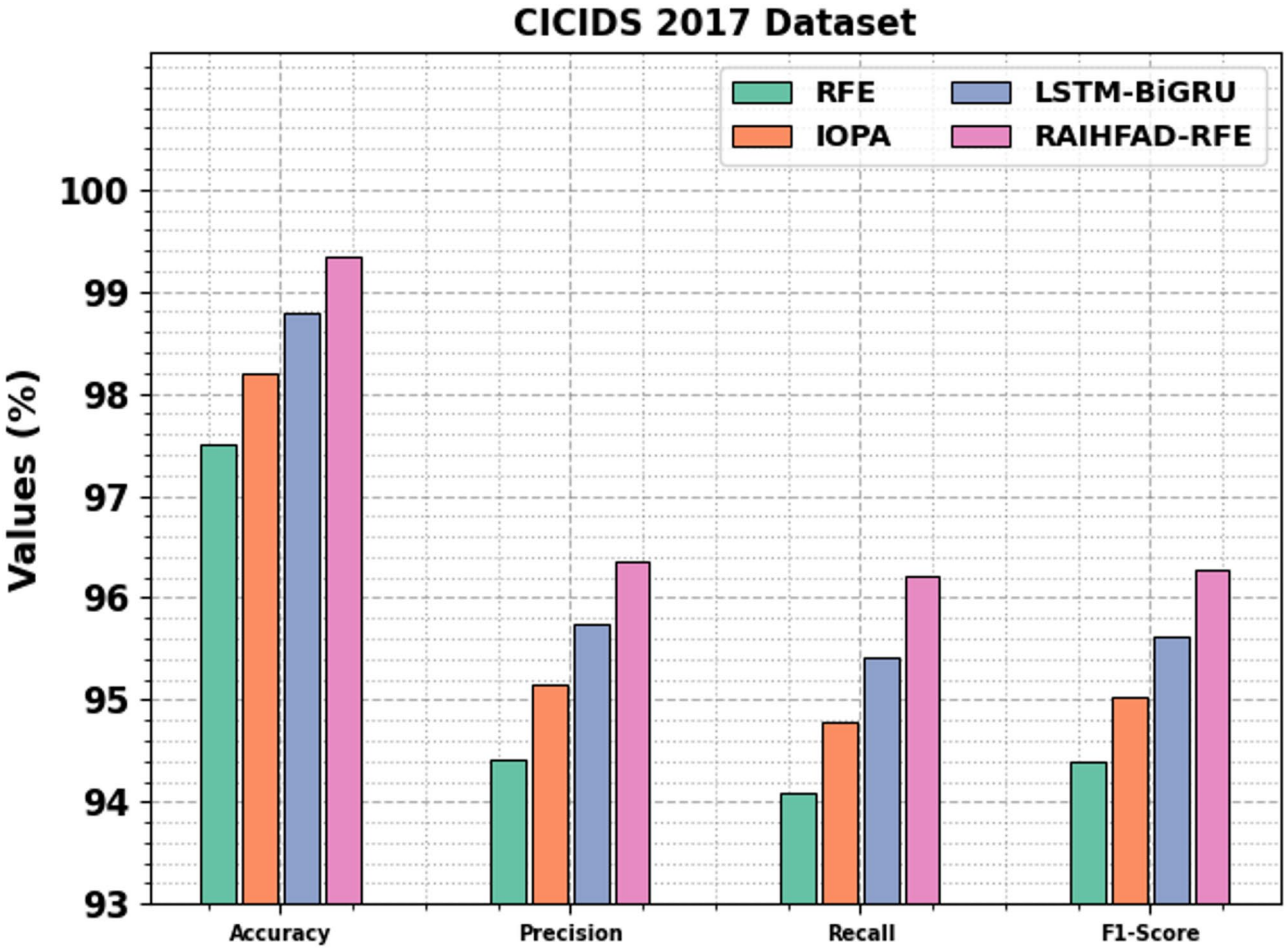

Fig. 8. Ablation study results comparing the RAIHFAD-RFE method on the CIC-IDS-2017 dataset.

Edge-IIoT Dataset			
S.no	**Type**	**Type of Event**	**Data Record**
1	**Benign**	"Normal"	4000
2	**Attacks**	"DDoS-UDP"	4000
3		"DDoS-ICMP"	4000
4		"SQL injection"	4000
5		"DDoS-TCP"	4000
6		"Password"	4000
7		"DDoS-HTTP"	4000
8		"Uploading"	4000
9		"Backdoor"	4000
10		"XSS"	4000
11		"Ransomware"	4000
12		"Fingerprinting"	4000
Total Record			48,000

Table 7. Details of the Edge-IIoT dataset.

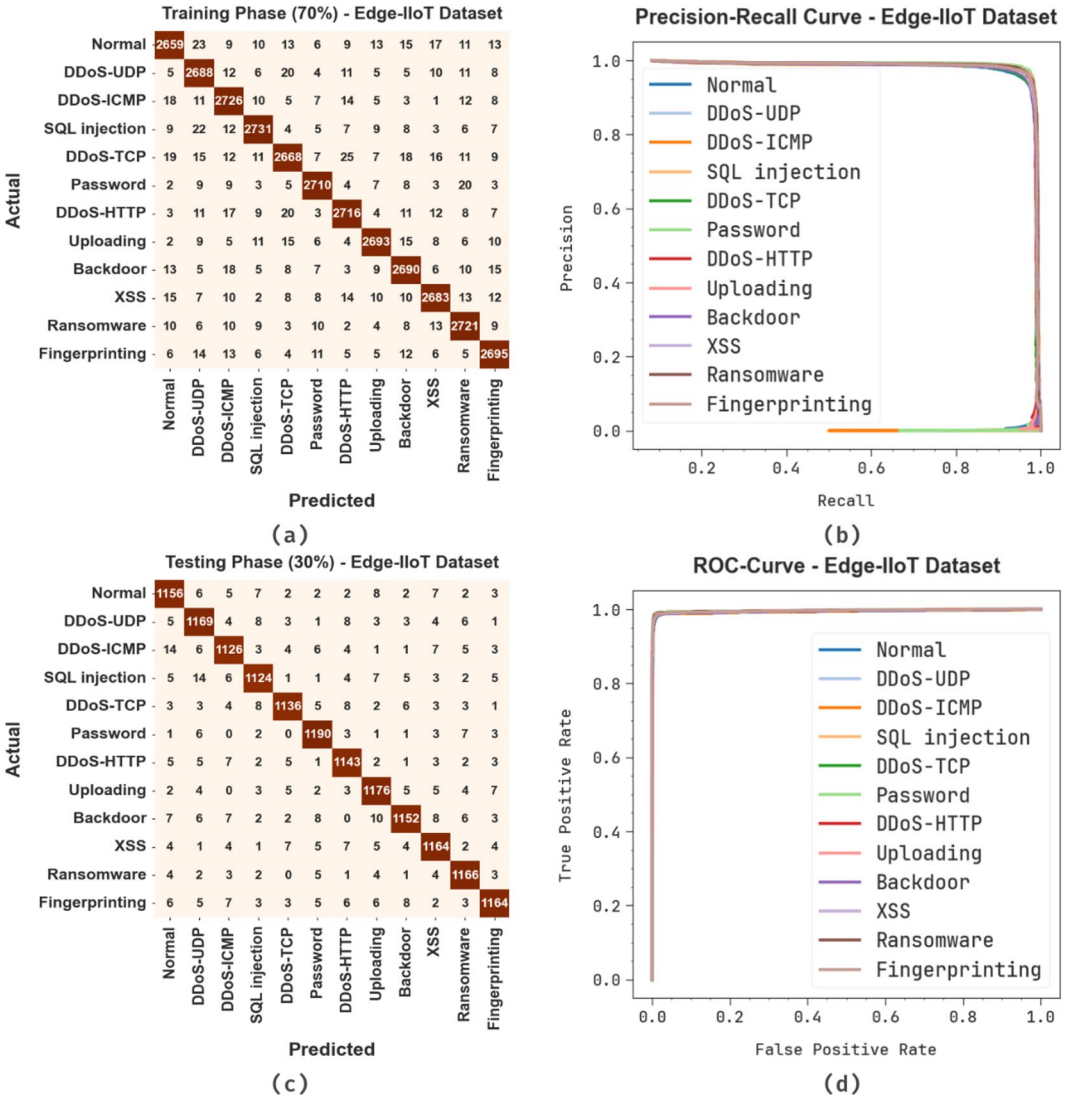

Fig. 9. Edge-IIoT dataset: (a, c) 70% and 30% confusion matrices and (b, d) PR and ROC curves.

Class Labels	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	MCC
TRPHE (70%)					
Normal	99.28	96.31	95.03	95.66	95.28
DDoS-UDP	99.32	95.32	96.52	95.91	95.54
DDoS-ICMP	99.34	95.55	96.67	96.10	95.75
SQL injection	99.48	97.08	96.74	96.91	96.63
DDoS-TCP	99.24	96.21	94.68	95.44	95.03
Password	99.56	97.34	97.38	97.36	97.12
DDoS-HTTP	99.40	96.52	96.28	96.40	96.07
Uploading	99.50	97.19	96.73	96.96	96.68
Backdoor	99.37	95.97	96.45	96.21	95.87
XSS	99.39	96.58	96.10	96.34	96.01
Ransomware	99.41	96.01	97.01	96.51	96.19
Fingerprinting	99.44	96.39	96.87	96.63	96.32
Average	**99.39**	**96.37**	**96.37**	**96.37**	**96.04**
TSPHE (30%)					
Normal	99.29	95.38	96.17	95.77	95.39
DDoS-UDP	99.28	95.27	96.21	95.74	95.35
DDoS-ICMP	99.30	95.99	95.42	95.71	95.33
SQL injection	99.35	96.48	95.50	95.99	95.63
DDoS-TCP	99.46	97.26	96.11	96.68	96.39
Password	99.53	96.67	97.78	97.22	96.97
DDoS-HTTP	99.43	96.13	96.95	96.54	96.23
Uploading	99.38	96.00	96.71	96.35	96.02
Backdoor	99.33	96.89	95.13	96.00	95.64
XSS	99.35	95.96	96.36	96.16	95.81
Ransomware	99.51	96.52	97.57	97.05	96.78
Fingerprinting	99.38	97.00	95.57	96.28	95.94
Average	**99.38**	**96.30**	**96.29**	**96.29**	**95.96**

Table 8. DDoS attack detection of the RAIHFAD-RFE technique on the Edge-IIoT dataset.

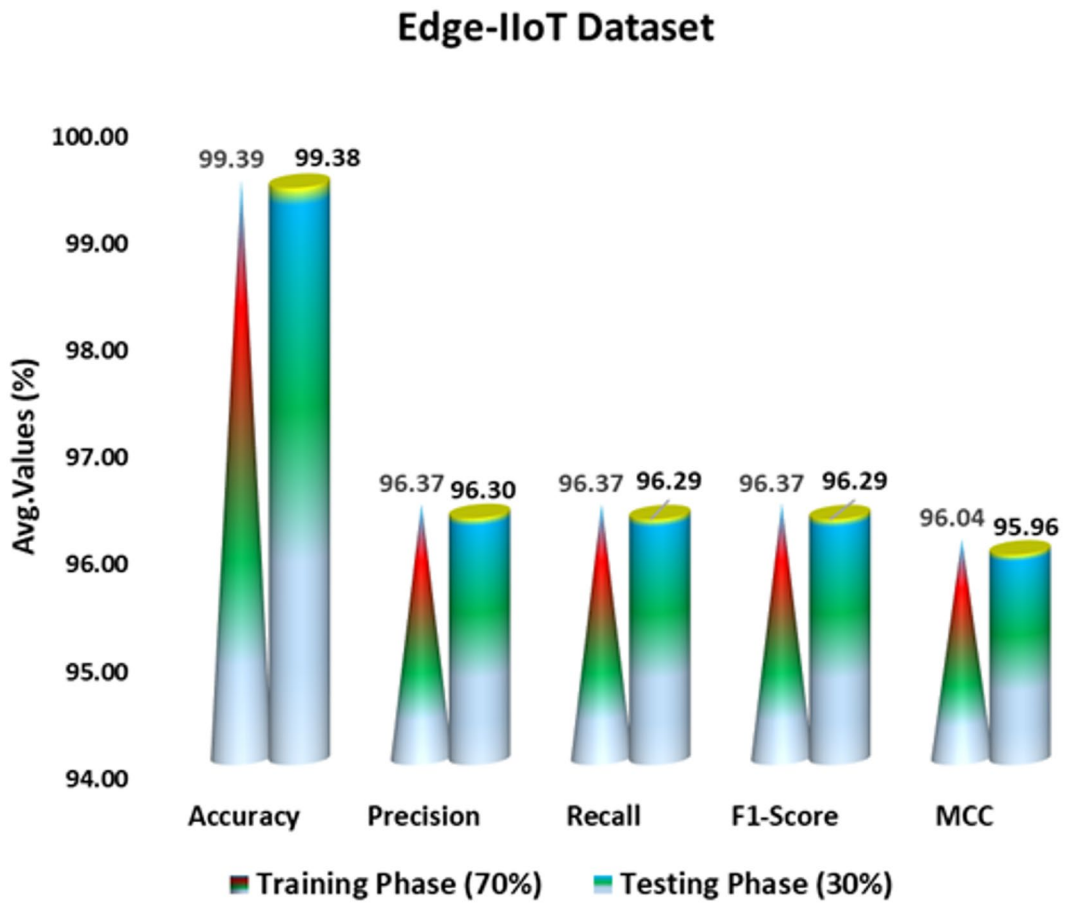

Fig. 10. Average values of the RAIHFAD-RFE model on the Edge-IIoT dataset.

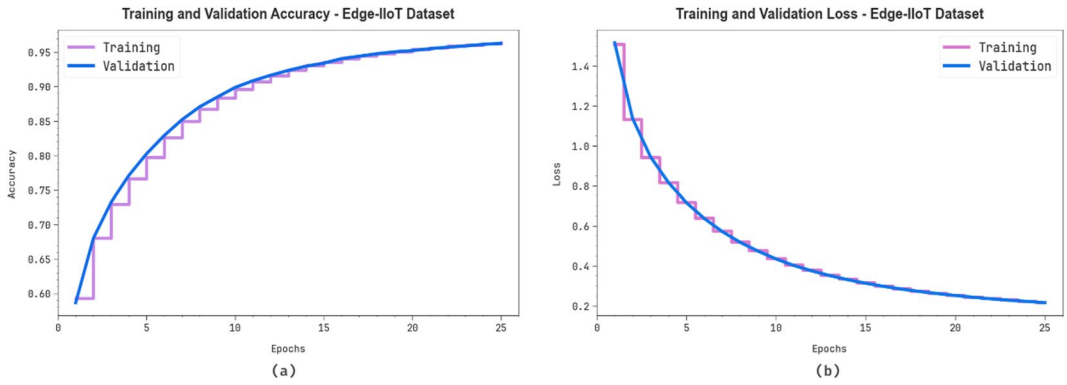

Fig. 11. (**a**) Accuracy and (**b**) loss curves on the Edge-IIoT dataset.

Edge-IIoT Dataset						
Method	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$	**Inference Latency (ms)**	**Memory Footprint (MB)**
Shallow ANN	93.36	93.73	87.11	96.16	17.96	560
Isolated LSTM	98.27	93.72	88.93	89.31	19.53	1003
CNN Classifier	96.90	93.15	79.47	95.61	10.68	363
RF Method	82.51	90.31	88.04	92.22	22.91	607
SVM Model	79.23	88.07	85.79	96.24	22.52	488
DNN Algorithm	96.38	91.85	79.60	93.40	10.21	429
Inception Time	96.60	80.81	89.26	94.69	22.08	402
RAIHFAD-RFE	99.39	96.37	96.37	96.37	7.63	328

Table 9. Comparative study of the RAIHFAD-RFE model on the Edge-IIoT dataset[43–45].

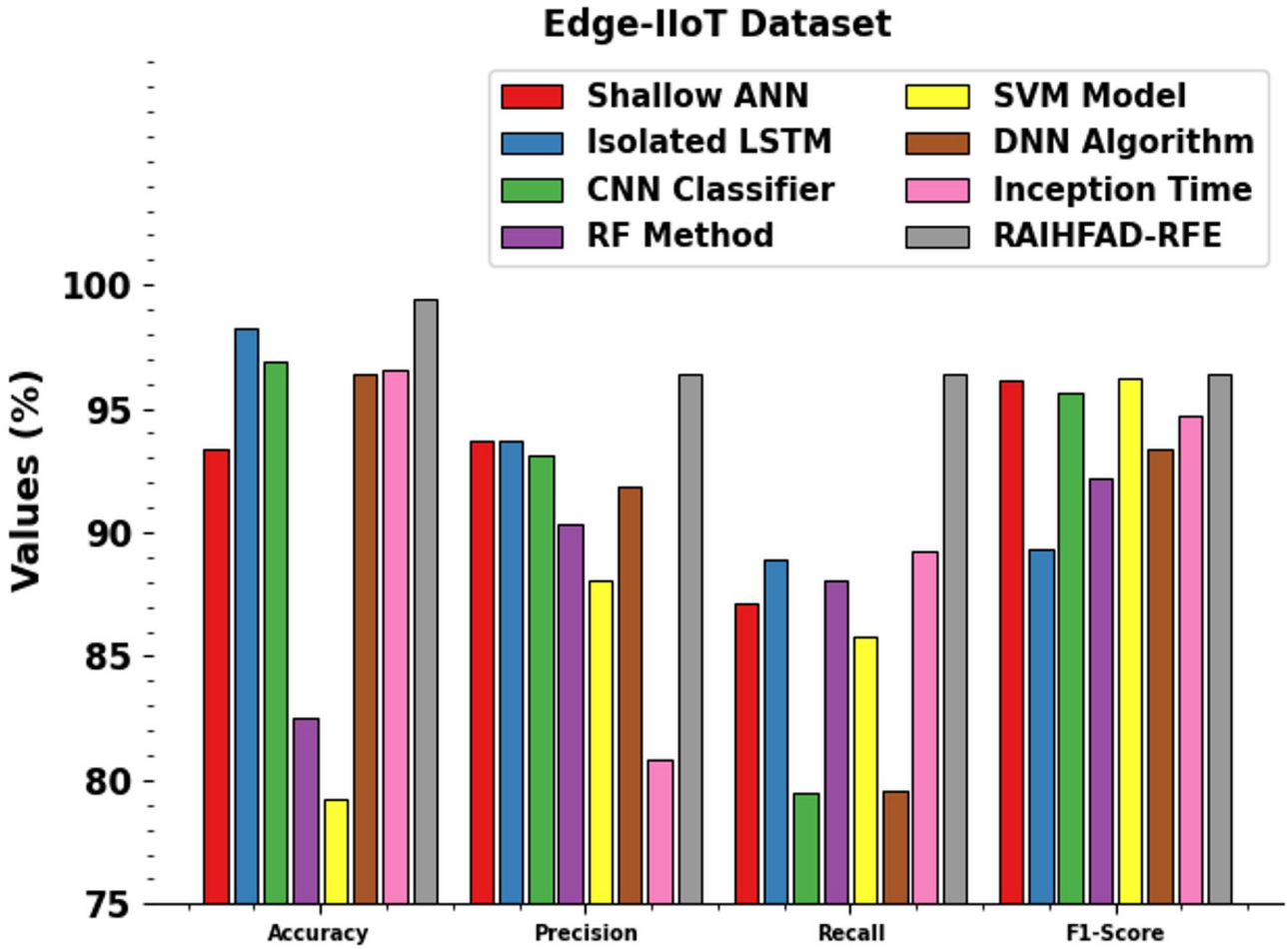

Fig. 12. Comparative analysis of the RAIHFAD-RFE model on the Edge-IIoT dataset.

Edge-IIoT Dataset				
Method	$Accu_y$	$Prec_n$	$Reca_l$	$F1_{Score}$
RFE	97.38	94.71	94.3	94.51
IOPA	98.14	95.35	95.08	95.16
LSTM-BiGRU	98.86	95.86	95.74	95.83
RAIHFAD-RFE	99.39	96.37	96.37	96.37

Table 10. Results of the ablation study of the RAIHFAD-RFE technique on the Edge-IIoT dataset.

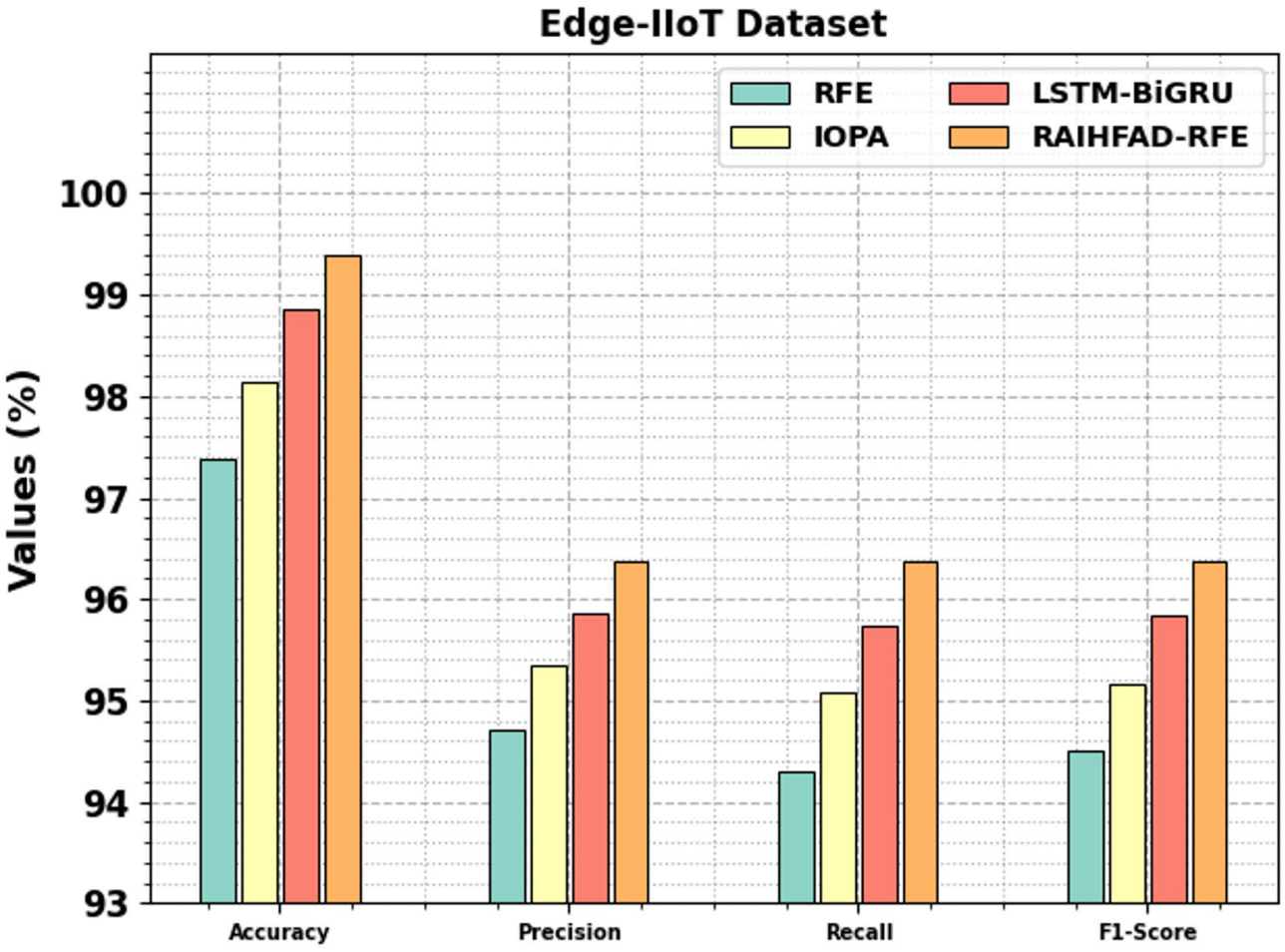

Fig. 13. Results of the ablation study of the RAIHFAD-RFE technique on the Edge-IIoT dataset.

Data availability

The data supporting the findings of this study are openly available in Kaggle datasets https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset and https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot, referenced as[41,42].

Received: 5 June 2025; Accepted: 3 October 2025
Published online: 10 November 2025

References

1. Ferdous, F. S., Biswas, T. & Jony, A. I. Enhancing cybersecurity: machine learning approaches for predicting DDoS attack. *Malaysian J. Sci. Adv. Technol.* **4**, 249–255 (2024).
2. Said, D. Quantum computing and machine learning for cybersecurity: Distributed denial of service (DDoS) attack detection on smart micro-grid. *Energies*, *16*(8), p.3572. (2023).
3. Balasubramaniam, S. et al. Optimization enabled deep learning-based ddos attack detection in cloud computing. *International Journal of Intelligent Systems*, *2023*(1), p.2039217. (2023).
4. Alshdadi, A. A. et al. Big data-driven deep learning ensembler for DDoS attack detection. *Future Internet*, *16*(12), p.458. (2024).
5. Said, D. Quantum computing and machine learning for cybersecurity: distributed denial of service (DDoS) attack detection on smart Micro-Grid. *Energies 2023*. **16**, 3572 (2023). doi. org/10.3390/en16083572.
6. Söğüt, E. & Erdem, O. A. A multi-model proposal for classification and detection of DDoS attacks on SCADA systems. *Applied Sciences*, *13*(10), p.5993. (2023).
7. Singh, S., Gupta, M. & Sharma, D. K. January. DDOS Attack detection with machine learning: a systematic mapping of literature. In *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 939–945). IEEE. (2023).
8. Tikhe, D., Deshpande, P., Wani, P., Mante, J. & Kolhe, K. August. Leveraging Metaheuristic Algorithms for Optimal Feature Selection in IoT Cybersecurity: A Study on Enhancing DDoS Attack Detection. In *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)* (pp. 1–6). IEEE. (2024).
9. Kumari, P. & Jain, A. K. December. Deep learning-powered multiclass classification of DDoS attacks on 6G-connected IoT devices. In *2023 International Conference on Modeling, Simulation & Intelligent Computing (MoSICom)* (pp. 614–618). IEEE. (2023).
10. Al-Hagery, M. A. & Abdalla Musa, A. I. Enhancing network security using possibility neutrosophic hypersoft set for cyberattack detection. *International J. Neutrosophic Sci. (IJNS)* **25**(1), 38–50 (2025).
11. Alrumaih, T. N. & Alenazi, M. J. A novel framework for enhancing the resilience of industrial networks against DDoS attacks with adaptive recovery. *Alexandria Eng. J.* **121**, 248–262 (2025).
12. Hu, T. & Shi, K. *Secure Synchronization Control for Complex Dynamic Networks with event-triggered Communication Strategy Under Multichannel denial-of-service Attacks* (ISA transactions, 2025).
13. Wang, H., Jia, N., He, Y. & Lian, Z. A new DDoS attack detection model based on improved stacked autoencoder and gated recurrent unit for software defined network. The Computer Journal, p.bxaf021. (2025).
14. Balamurugan, R. et al. January. Implementation of an effective methodology to avoid ddos attacks using cybersecurity norms. In 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) (pp. 1–6). IEEE. (2024).
15. Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J. & Sugali, M. N. DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, p.103661. (2024).
16. Martinez, F. et al. July. Redefining DDoS Attack Detection Using A Dual-Space Prototypical Network-Based Approach. In 2024 33rd International Conference on Computer Communications and Networks (ICCCN) (pp. 1–9). IEEE. (2024).
17. Ahmed, A., Awaıs, M., Sıraj, M. & Umar, M. Enhancing cybersecurity with trust-based machine learning: A defense against ddos and packet suppression attacks. The Eurasia Proceedings of Science Technology Engineering and Mathematics, 23, pp.262–268. (2023).
18. Hossain, M. A. & Islam, M. S. December. An ensemble-based machine learning approach for botnet-based DDoS attack detection. In 2023 IEEE International Conference on Telecommunications and Photonics (ICTP) (pp. 1–5). IEEE. (2023).
19. Emirmahmutoğlu, E. & Atay, Y. A feature selection-driven machine learning framework for anomaly-based intrusion detection systems. *Peer-to-Peer Netw. Appl.* **18** (3), 1–28 (2025).
20. Behiry, M. H. & Aly, M. Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. *Journal of Big Data*, *11*(1), p.16. (2024).
21. Farid, A. A. & Khalil, A. T. Optimizing WSN security: an advanced ML-Driven intrusion detection system with SMOTE-Tomek. *Int. J. Telecommunications*. **5** (01), 1–28 (2025).
22. AboulEla, S., Ibrahim, N., Shehmir, S., Yadav, A. & Kashef, R. Navigating the cyber threat landscape: an in-depth analysis of attack detection within IoT ecosystems. *Ai* **5** (2), 704–732 (2024).
23. Luthfi, A. F. et al. Enhancing software defect prediction: HHO-Based wrapper feature selection with ensemble methods. *Indonesian J. Electron. Electromedical Eng. Med. Inf.* **7** (2), 188–202 (2025).
24. Al-Amiedy, T. A., Anbar, M. & Belaton, B. OPSMOTE-ML: an optimized SMOTE with machine learning models for selective forwarding attack detection in low power and lossy networks of internet of things. *Cluster Comput.* **27** (9), 12141–12184 (2024).
25. Thamer Francis, G., Souri, A. & İnanç, N. A hybrid firefly-based attribute selection and split-point mechanism for Securing software-defined industrial internet of things. *J. High Speed Netw.* **31**, 09266801251338138 (2025).
26. Kocyigit, E., Korkmaz, M., Sahingoz, O. K. & Diri, B. Enhanced feature selection using genetic algorithm for machine-learning-based phishing URL detection. *Applied sciences*, *14*(14), p.6081. (2024).
27. Qiao, C., Zeng, Y., Lu, H., Liu, Y. & Tian, Z. An efficient incentive mechanism for federated learning in vehicular networks. *IEEE Netw.* **38** (5), 189–195 (2023).
28. Alfatemi, A. et al. Identifying distributed denial of service attacks through multi-model deep learning fusion and combinatorial analysis. *Journal of Network and Systems Management*, *33*(1), p.8. (2025).
29. Lv, Y., Shi, W., Zhang, W., Lu, H. & Tian, Z. Do not trust the clouds easily: the insecurity of content security policy based on object storage. *IEEE Internet Things J.* **10** (12), 10462–10470 (2023).
30. Al-Shukaili, N. A., Kiah, M. L. M. & Ahmedy, I. Optimizing feature selection and deep learning techniques for precise detection of low-rate distributed denial of service (LDDoS) attack. *Discover Internet of Things*, *5*(1), p.80. (2025).
31. Lu, H. et al. AutoD: intelligent blockchain application unpacking based on JNI layer deception call. *IEEE Netw.* **35** (2), 215–221 (2020).
32. Pradeesh, S., Jeyakarthic, M. & Thirumalairaj, A. Enhanced Hybrid Approach for Multi-Class DDoS Attack Detection and Classification in Software-Defined Networks Using Remote Sensing and Data Analytics. *Remote Sensing in Earth Systems Sciences*, pp.1–15. (2025).
33. Lu, H. et al. DeepAutoD: research on distributed machine learning oriented scalable mobile communication security unpacking system. *IEEE Trans. Netw. Sci. Eng.* **9** (4), 2052–2065 (2021).
34. Dilshad, M., Syed, M. H. & Rehman, S. Efficient distributed denial of service attack detection in internet of vehicles using Gini index feature selection and federated learning. *Future Internet*, *17*(1), p.9. (2025).

35. Gu, Z. et al. Gradient shielding: towards Understanding vulnerability of deep neural networks. *IEEE Trans. Netw. Sci. Eng.* **8** (2), 921–932 (2020).
36. Asuai, C. et al. Enhancing DDoS detection via 3ConFA feature fusion and 1D convolutional neural networks. *J. Future Artif. Intell. Technol.* **2** (1), 145–162 (2025).
37. Fu, N., Lee, J. H., Liu, J., Lee, S. & Kim, M. K. Electricity Demand Forecasting for Cultural Institutions: A Comparative Study of Lstm and Cnn-Lstm Models with Three Data Normalization Techniques Using Weather and Price Data–Case Studies from Norwegian Museums. *Available at SSRN 5262024*.
38. Akinola, D., Ajinaja, M. O. & Adewuyi, J. A. *Machine Learning-Based Network Intrusion Detection for IOT and Smart Detection Using Recursive Feature Elimination* (Binning Technique and Grid Search CV, 2024).
39. Yan, X., Mao, X., Li, M. & Wang, X. Hybrid Esc-Lstm-Bigru Deep Learning Model for Multi-State Estimation of Lithium-Ion Batteries.
40. Yang, J. & Safarzadeh, J. Using BERT and ZFNet/ELM optimized by improved Orca optimization algorithm for sentiment analysis. *Scientific Reports*, *15*(1), p.15238. (2025).
41. https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset
42. https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot
43. Dash, N. et al. An optimized LSTM-based deep learning model for anomaly network intrusion detection. *Scientific Reports*, *15*(1), p.1554. (2025).
44. Mansour, R. F. Artificial intelligence based optimization with deep learning model for blockchain enabled intrusion detection in CPS environment. *Scientific Reports*, *12*(1), p.12937. (2022).
45. Alblehai, F. Artificial intelligence-driven cybersecurity system for internet of things using self-attention deep learning and metaheuristic algorithms. *Scientific Reports*, *15*(1), p.13215. (2025).

Author contributions

Conceptualization, Data curation and Formal analysis, Investigation and Methodology, Funding Support, Project administration and Resources: Supervision;, Validation and Visualization, Writing—original draft - Sultan Alkhliwi.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.