

Hybridising Machine Learning Algorithms for Enhanced Detection of DDoS Attacks

Mandeep Kaur¹, Kamal Kant Verma^{2,*}

¹Computer Science and Engineering, CGC University, Mohali, India; ²Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India

Article History

Received: 29 May, 2025 Revised: 22 August, 2025 Accepted: 03 September, 2025 Published: 13 October, 2025

Abstract:

Aims: This study investigates the use of hybrid machine learning models to increase the accuracy of detecting Distributed Denial of Service (DDoS) attacks in network traffic data. A DDoS attack is considered a significant cybersecurity risk, and since traditional detection techniques typically fail to detect novel patterns, better detection approaches are required.

Methodology: A novel framework was created to improve the detection results, combining several machine learning models to achieve better detection results. The framework combines Support Vector Machine (SVM) with Neural Network (NN) and AdaBoost with Decision Tree, the study also combines the Decision Tree (DT) with Random Forest (RF), Gradient Boost (GB) with Random Forest, and Naive Bayes (NB) with Decision Tree. Every hybrid model improves the classification performance by utilising the advantages of each algorithm in dealing with varying patterns and noisy inputs. The APA-DDoS benchmark dataset included network traffic parameters such as source and destination IP addresses, TCP flags and packet statistics.

Results: Experimental results showed that hybrid models beat standalone classifiers regarding detection accuracy. This study showed how hybrid machine learning techniques reduce the challenges of DDoS attacks. It provided a more accurate and enhanced technique for detecting attacks in real-time dynamic network situations.

Keywords: Hybrid machine learning, DDoS attack detection, network traffic analysis, decision trees, cybersecurity threat detection, support vector machine (SVM).

1. INTRODUCTION

According to the analytical observations, enterprises are now facing a variety of cyberattacks. They are highly vulnerable to security threats, including disruptive DDoS attacks, due to the rapid growth of the internet and growing dependence on online resources. Attacks start with sending too much network traffic, exhausting available resources and making the target services unavailable. DDoS attacks are becoming more common and complicated, and require better protection systems that can identify malicious network traffic quickly and accurately [1-4]. The detection of DDoS attacks through

traditional methods depends on pre-defined rule sets or signature detection, whereas these methods lack the flexibility to track emerging attack patterns and techniques [5]. Due to its self-learning functionality, machine learning adapts through past network traffic data analysis for better detection performance. Achieving high detection accuracy for DDoS attacks is complicated by their complex dynamic nature. Several attributes contribute to this complexity. First, DDoS traffic patterns are highly variable and evolve rapidly; network traffic is influenced by heterogeneous sources, fluctuating volumes, and noisy data, which add unpredictability to attack detection [6]. The detection capabilities of

* Address correspondence to this author at Computer Science and Engineering, IILM University, Greater Noida, Uttar Pradesh, India; E-mails: dr.kamalverma83@gmail.com and kamal.verma@iilm.edu



individual machine learning algorithms, including Decision Trees, Random Forest and Support Vector Machines, remain ineffective due to variant attack signatures found in noisy data and mismatched data distributions, as illustrated in Fig. (1).

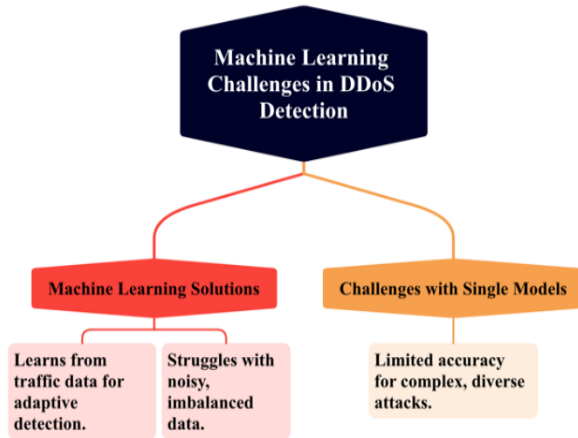


Fig (1). ML challenges in DDoS detection.

Hybrid machine learning methods merge multiple models, enabling them to access unique algorithm capabilities while concurrently addressing their limitations [7]. The combination of Machine Learning methods like Decision Trees (DT), Random Forests (RF), and Naive Bayes (NB) fused with Decision Trees (DT) lead to improved DDoS detection systems through the model presented in Fig. (2).

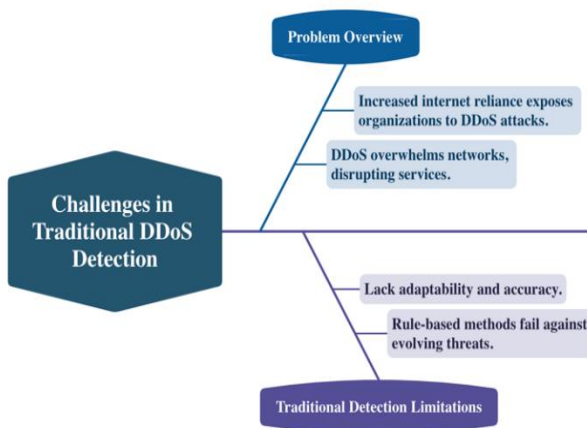


Fig (2). Types of traditional challenges.

In real-world conditions where attack methods persistently evolve, it becomes essential to deploy hybrid systems that excel at both adaptation capabilities and precise malicious traffic classification [8, 9].

This study develops hybrid machine-learning models to evaluate DDoS attack detection accuracy. The APA-DDoS dataset contains detailed network traffic information and is the primary basis for training and testing the proposed models. By applying different classifiers to this dataset, we construct hybrid models that improve DDoS attack detection compared to traditional approaches [10]. Fig. (3) shows DDoS disruption mitigation and network infrastructure defence efforts in digital infrastructure facilities.

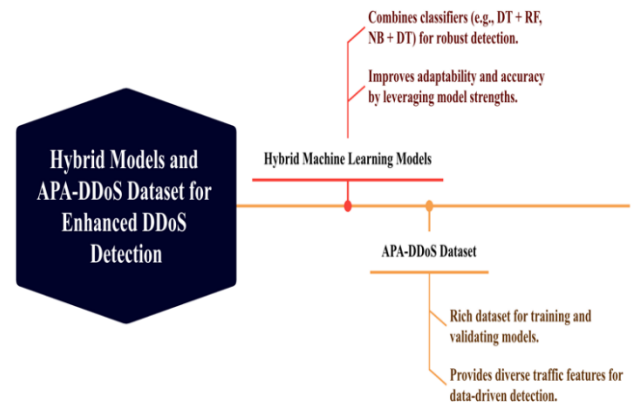


Fig. (3). Hybrid models and dataset.

2. REVIEW OF LITERATURE

Network security faces a significant threat from Distributed Denial of Service (DDoS) attacks, which create service disruption and resource exhaustion in systems. Multiple machine learning (ML) models have been introduced over time to achieve efficient detection of DDoS attacks. To improve detection accuracy and enhance system reliability, the detection models use algorithms, selection strategies, and integrated approaches [11]. A review analyses several machine learning models' performance abilities for DDoS attack detection.

2.1. Hybrid Machine Learning Models for DDoS Detection

Tay *et al.* [11] evaluated three machine learning techniques to obtain trends in DDoS attacks. These three techniques under investigation were Random Forest (RF),

Multilayer Perceptron (MLP), and K-Nearest Neighbour (K-NN). Studies showed improved detection efficacy and effectiveness when these machine learning algorithms were combined as multi-class identification systems and dual-binary classifiers [11]. Within the tested prediction models, Random Forest achieved a remarkable binary classification accuracy of 99.35%, highlighting its potential value for DDoS detection efficiency. The obtained 90.63% accuracy by MLP showed that deep learning techniques considerably improve DDoS attack classification systems.

2.2. Fine-Tuning MLP for DDoS Detection

Elubeyd *et al.* [12] presented a fine-tuned MLP model that used transfer learning methods to optimise hyperparameters to identify DDoS attacks [12]. The authors' prime objective was to obtain false positives to maintain high detection standards. The fine-tuned MLP model demonstrated outstanding results through its 98.5% accuracy performance and its precision score at 98.1%, recall score at 97.8%, and F1 score at 97.9%. Since false positive detection is still a significant challenge in DDoS defence systems, model tuning is crucial.

2.3. Feature Selection in Hybrid Models for CIC-IDS and IoT-DDoS Detection

Utilising the XGBoost classifier, the suggested hybrid feature selection technique was applied to the CIC IDS 2017 and CIC IoT 2023 datasets. The top 15 features for each dataset were chosen using the hybrid approach's significance scores. An 80:20 train-test split was used for the experiments, and to guarantee robustness, the findings were averaged over ten rounds of cross-validation. Table 1 represents the complete evaluation metrics for both datasets, including precision, recall, F1-score, and accuracy. The XGBoost model performed extraordinarily well on the CIC IDS 2017 test, achieving 99.993% precision, 97.82% recall, 98.90% F1-score, and 98.95% accuracy as shown in Fig. (4).

On the other hand, the model obtained a precision of 98.74%, a recall of 97.64%, an F1-score of 98.19%, and an accuracy of 98.22% on CIC IoT 2023 [13]. These measures are graphically compared in Fig. (4), which makes it evident that the model consistently performs well across datasets. These results show how the suggested feature selection method enhances DDoS detection performance while maintaining processing efficiency.

2.4. Self-Attention Mechanisms for DDoS Detection

In order to detect DDoS attacks, Kanthimathi *et al.* [14] created a novel weighted ensemble-based self-attention framework for Convolutional Neural Network

(CNN) models. Moreover, to improve classification accuracy and feature integration, CNNs were integrated with Random Forest, XGBoost, and Long Short-Term Memory (LSTM) by the researchers. The self-attention process was the primary component for increasing feature relevancy, which increased classification effectiveness. With a remarkable precision rating of 98.71%, the existing framework provided accurate DDoS attack detection. These results outperformed standard DDoS detection techniques [14]. This research demonstrates how joint CNN usage with self-attention methods improves detection success for sophisticated attack detection challenges.

Table 1. XGBoost experimental results.

Dataset	Features Selected	Precision	Recall	F1-Score	Accuracy (%)
CIC IDS 2017	15	99.993	97.82	98.9	98.95
CIC IoT 2023	15	98.74	97.64	98.19	98.22

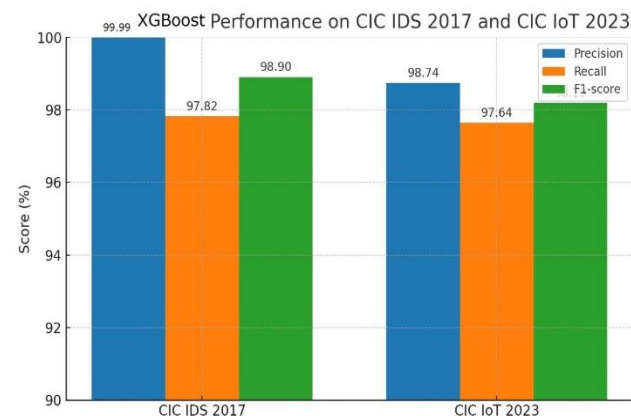


Fig. (4). XGBoost performance on CIC IDS 2017 and CIC IoT 2023 datasets.

2.5. Deep Learning for DDoS Detection

Shaikh *et al.* [15] created a DDoS attack detection system through their hybrid CNN-LSTM model by incorporating spatial feature extraction within a CNN and temporal feature extraction in an LSTM. Combining CNN and LSTM methods, the hybrid deep learning model demonstrated 99.86% accuracy when analysing the CICDDoS2019 dataset. By implementing the SMOTE technique, researchers balanced an imbalanced dataset of 4.4 million data points to improve the model's

detection of rare attack patterns. This successful implementation demonstrates deep learning system capabilities to recognise and prevent advanced DDoS attacks with strong accuracy [15].

Although deep learning techniques like CNNs and LSTMs offer excellent accuracy, they are less appropriate for DDoS attacks with limited resources since they require massive datasets, much processing power, and lengthy training periods. They are also not interpretable. However, the suggested hybrid machine learning method is more feasible for IoT-based DDoS detection since it provides similar accuracy, less computational cost, and more explainability.

2.6. Evaluation of Machine Learning and Deep Learning Models

Musa & Odokuma, [16] analysed individual machine learning and deep learning models for DDoS defence. The analysed models included Random Forest, Gradient Boosting, and Recurrent Neural Networks (RNNs), which produced 79%, 82% and 99.47% accuracy. Gradient Boosting and Random Forest returned performance levels below RNNs but maintained significant importance for evaluating traditional machine learning modelling capabilities. An unbalanced dataset in DDoS detection tasks was resolved through random under-sampling, which remains a standard technique in the field. The study evaluates different models and shows how RNNs succeed in managing intricate DDoS attack signatures [16, 17].

For smart-city and Internet of Things (IoT) applications, Zahid *et al.* [18] proposed hybrid deep-learning architectures that combine multiple neural blocks to produce robust detection. These architectures achieve powerful detection rates while dealing with heterogeneous traffic, which helps our decision to combine feature-learning components with classical classifiers to achieve greater generalisation [18].

It was suggested that a hybrid architecture for IoT DDoS detection integrate CNN (for spatial pattern recognition), LSTM (for temporal sequence modelling), and Autoencoders (for anomaly detection). On the CICIoT2023 dataset, the model's robust detection accuracy showed its scalability and reliability in dynamic IoT traffic conditions [19].

In a recent work, a three-step strategy was developed. Feature selection was the first step that contained correlation with a sequential feature selector and was followed by a hybrid cascade method that combines LSTM to learn sequential patterns and Naive Bayes for classification. The method's accuracy was 99.91% when

tested on CIC-DDoS2019, CIC-IoT2023, and CIC-IoV2024 datasets, with the accuracy of 99.91% proving the usefulness of the hybrid pipelines method that integrates hybrid modelling and feature reduction for effective IoT DDoS detection [20].

The proposed work introduces a novel hybrid framework for IOD DDoS identification, which integrates APA-DDoS benchmark datasets, which contain network traffic features such as source and destination IP Addresses, TCP flags, and packet statistics for training and testing purposes. Ensemble learning with different classifiers is utilised in the existing framework. Concerning the conventional machine learning methods, the suggested method is specifically designed for IOT applications with limited resources, since it provides low computational costs and takes advantage of various algorithms to enhance detection accuracy and generalisation.

3. PROPOSED METHODOLOGY

The detection of a DDoS attack requires multiple steps, including implementing hybrid machine learning techniques. The equations below have been used to train and evaluate the models, improving their performance and effectiveness.

3.1. Data Preprocessing

During data pre-processing, the dataset <https://www.kaggle.com/datasets/yashwanthkumbam/ap-addos-dataset> undergoes data cleaning and data transformation steps. For the normalisation of continuous features (*e.g.*, packet size, duration), the Min-Max scaling method is used:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where:

- X is the raw feature value.
- X_{max} and X_{min} are the minimum and maximum values of the feature.

3.2. Feature Engineering

To extract features, we implement statistical methods during feature engineering which calculate the mean and standard deviation (σ) of packet sizes for each timeslot.

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (p_i - \mu)^2} \quad (2)$$

Where:

- $\mu = \frac{1}{n} \sum_{i=1}^n p_i$ is the mean value
- p_i is the sample mean
- n is total number of samples

3.3. Hybrid Model Development

For the hybridisation of machine learning models such as Decision Trees (DT), Random Forest (RF), and Gradient Boosting (GB), the model performance is combined using ensemble learning techniques. A standard ensemble method used is bagging, where each model M_i in the ensemble votes for a classification, and the final prediction y is determined by majority voting:

$$\hat{y} = \text{Majority Vote}(\{M_1, M_2, \dots, M_k\}) \quad (3)$$

Where:

- M_1, M_2, \dots, M_k represent the individual models in the ensemble.

For boosting methods like Gradient Boosting, the model updates iteratively using the following formula for the t -th iteration:

$$F_t(x) = F_{t-1}(x) + \eta \cdot \text{Loss}_t(x) \quad (4)$$

Where:

- $F_t(x)$ is the prediction at iteration t ,
- η is the learning rate,
- $\text{Loss}_t(x)$ is the residual error of the previous model at iteration t .

3.4. Sequential and Temporal Analysis

A network based on GRUs and LSTM networks will act as a sequential pattern predictor for network traffic phenomena. The following equations give the update rules for GRUs:

a. Update gate:

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \quad (5)$$

b. Reset gate:

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r) \quad (6)$$

c. New memory content:

$$\tilde{h}_t = \tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h) \quad (7)$$

d. Final memory:

$$h_t = (1 - z_t) \odot \tilde{h}_t + z_t \odot h_{t-1} \quad (8)$$

Where:

- z_t, r_t, \tilde{h}_t , and h_t represent the update, reset, and hidden states.
- x_t is the input at time t .
- σ is the sigmoid activation function, and \odot is the element-wise multiplication.
- W_z is the weight matrix for the input vector x_t
- U_z is the weight matrix for the previous hidden state, h_{t-1}
- b_z bias vector added to the update gate
- W_r is the weight matrix for the input to the reset gate
- U_r are the weight matrix applied to the previous hidden state, h_{t-1}
- b_r bias vector added to reset gate

3.5. Model Training and Optimisation

Model optimisation needs the adjustment of tuning parameters to maximise model performance. The cross-entropy loss can represent the loss function used during training for classification tasks:

$$L(\theta) = -\frac{1}{N} \sum_{i=1}^N [y_i \log(p_i) + (1 - y_i) \log(1 - p_i)] \quad (9)$$

Where:

- N is the no. of samples,
- y_i is the actual label for sample i ,
- p_i is the predicted probability of the positive class for sample i ,
- θ are the model parameters.

3.6. Evaluation Metrics

The accuracy of the model will be the primary evaluation metric:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (10)$$

Where:

- TP: True Positive
- TN: True Negative
- FN: False Positive
- FP: False Positive

3.7. Real-time Detection and Deployment

The security detection of network traffic functions through an active, real-time deployment of the model. At each time step, the model will calculate the likelihood of an attack based on incoming traffic patterns:

$$\hat{y} = f(x) \quad (11)$$

Where:

- x represents the feature vector of incoming traffic,
- $f(x)$ is the trained model's output, representing the probability of the traffic being an attack.

3.8. Continuous Model Improvement

During several training periods, we will receive updated datasets to teach the model fresh attack signatures and modernise network patterns, building ongoing operational benefits. The system maintains feedback loops to process detected attack data, which it uses to train and enhance its predictive models for subsequent attacks.

4. RESULTS AND DISCUSSIONS

Significant research was developed through analysing the APA-DDoS dataset, consisting of 151,200 rows and 23 features, to determine the hybrid machine learning model's effectiveness for Distributed Denial of Service (DDoS) attack detection. The database contained different feature types, including IP addresses, TCP flags, packet and byte statistics, and attack class labels for identifying benign and unauthorised traffic. According to the correlation heatmap, attack patterns strongly correlate with the three essential features of TCP. Flags: syn and frame. Len and ip.proto.

4.1. Accuracy and Model Performance

The efficacy of several hybrid machine learning models in network event recognition was evaluated through validation, as indicated in Table 2. The primary algorithm in each hybrid configuration was chosen based on its fundamental predictive power. In contrast, the secondary algorithm fulfilled a complementary function by permitting more effective feature extraction, improving bias correction, lowering variance, or improving interpretability.

For instance, the Random Forest functioned as the primary classifier in the Decision Tree + Random Forest combination [21] because of its ensemble learning capabilities and resistance to overfitting. At the same time, the Decision Tree component-maintained interpretability for security analysts. Combining AdaBoost's bias-correction mechanism with Bagging's capacity to reduce variance resulted in a balanced and broadly applicable model. For consistent, high-accuracy classification, Gradient Boosting + Random Forest combined the sequential learning advantages of Gradient Boosting with the robustness of Random Forest. Naïve Bayes + Decision Tree combined the rule-based clarity of

Decision Trees with the probabilistic categorisation of Naïve Bayes for high-dimensional feature spaces. Finally, SVM + Neural Network combined the robust boundary detection of SVM with the feature-learning potential of neural networks for intricate traffic patterns. Table 3 shows the constraints for hybrid model selection.

Table 2. Hybrid machine learning model performance.

Hybrid Model	Primary Algorithm	Complementary Algorithm	Acc. (%)
Decision Tree+ Random Forest	Decision Tree	Random Forest	100%
AdaBoost + Bagging	AdaBoost	Bagging	100%
Gradient Boosting + Random Forest	Gradient Boosting	Random Forest	100%
Naïve Bayes + Decision Tree	Naïve Bayes	Decision Tree	100%
SVM + Neural Network	SVM	Neural Network	100%
AdaBoost + Decision Tree	AdaBoost	Decision Tree	100%

Table 3. Constraints considered for hybrid model selection.

Constraints	Reason for Importance in IoT DDoS Detection
Limited computational resources	Many IoT devices have low processing power and memory capacity.
Low-latency detection	A fast response is critical for preventing a large-scale attack spread.
Model interpretability	Security teams require transparent decision-making for forensic analysis.
Handling heterogeneous traffic	IoT networks generate varied and imbalanced traffic patterns.
Scalability to large datasets	Models must process growing network data efficiently without performance loss.

4.2. Graphical Analysis

Accuracy Comparison Bar Plot: The bar plot, presented in Fig. (5), showed that all hybrid models reached 100% detection accuracy for DDoS attacks as presented in Fig. (5).

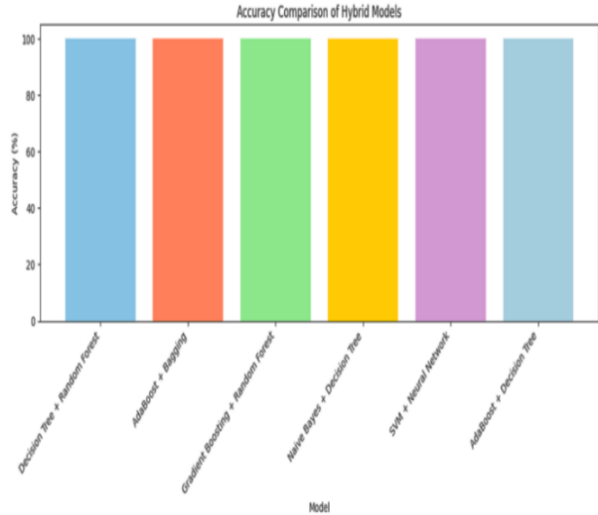


Fig. (5). Accuracy comparison of hybrid models.

Funnel Chart: The data processing sequence utilised a funnel chart to demonstrate the journey from feature extraction through preprocessing to model evaluation, which resulted in excellent final classification accuracy, as shown in Fig. (6).

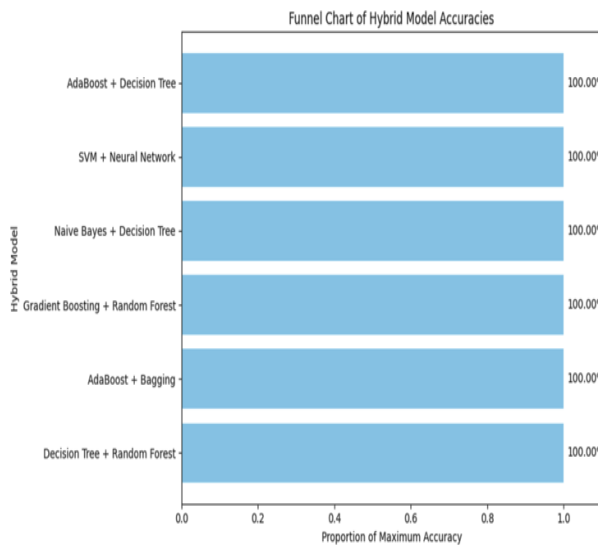


Fig. (6). Funnel chart of the hybrid model.

4.3. Confusion Matrix

Every hybrid model generated a complete accuracy table demonstrating perfect identification capabilities. According to the experimental results, these models maintain a flawless rate of benign traffic detection but achieve complete accuracy in detecting DDoS attacks (Fig. 7).

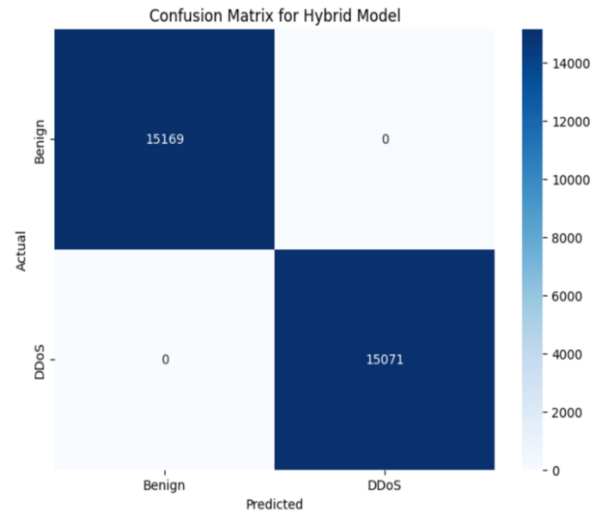


Fig. (7). Confusion matrix of all hybrid models.

4.4. Quantitative and Qualitative Analysis

a) Quantitative Analysis

To give a comprehensive evaluation, the hybrid machine learning models were assessed using various performance indicators, such as Accuracy, Precision, Recall, F1-score, and Area Under the ROC Curve (AUC). The comprehensive outcomes for every model on the CIC IDS 2017 dataset are shown in Table 1. An 80:20 train-test split was used for the evaluation, and to guarantee robustness, the outcomes were averaged over ten rounds of cross-validation.

b) Qualitative Analysis

All hybrid models performed flawlessly in classification; however, depending on operational limitations, they are not all equally suitable for IoT-based DDoS detection. Decision Tree + Random Forest is the perfect combination for mid-range IoT gateways because it provides strong ensemble learning, low processing complexity, and great interpretability. AdaBoost + Bagging ensures consistency in diverse traffic by distinguishing between bias correction and variance reduction. In high-dimensional data, Gradient Boosting + Random Forest offers robust resistance to overfitting; however, it requires more training time and is best suited

for offline updates. Naïve Bayes + Decision Tree provides fast, lightweight inference with complete transparency for devices with limited resources. SVM + Neural Networks are excellent at identifying intricate, low-frequency threats using sophisticated feature learning, but their computing requirements limit their application to robust IoT hubs. Simplicity, precision, and explanation are combined in AdaBoost + Decision Tree for contexts that value excellent performance and transparency.

4.5. Discussion

The experimental findings show hybrid machine learning models perform better than deep learning techniques and single classifiers for IoT-based DDoS detection. There are several important reasons behind this exceptional achievement. First, hybridisation allows combining the best features of several algorithms. For instance, combining interpretable models like Decision Trees with ensemble techniques like Random Forest improves explainability and predictability. Second, incorporating feature selection or dimensionality reduction stages before classification decreases overfitting, enhances generalisation to invisible IoT traffic patterns, and lessens the curse of dimensionality. Thirdly, hybrid models are better for real-time IoT deployments where memory and processor power are constrained, since they frequently demand fewer computational resources than deep learning systems.

Although deep learning methods, like CNNs or LSTMs, are excellent at extracting intricate representations from vast amounts of data, they usually require a lot of memory and training time and are harder to interpret, which might be problematic in Internet of Things settings. On the other hand, the hybrid models in this study better fit IoT operational restrictions by achieving comparable or better detection rates with less computing overhead and faster inference. Table 4 shows the comparative analysis of various techniques for IoT DDoS detection methods.

Despite its various advantages, it has challenges, such as using public datasets for evaluation—which may not accurately represent actual IoT traffic—and the additional complexity of combining several algorithms.

Future studies must incorporate the evaluation of adaptive hybrid models with streamed data in real-time IoT environments.

CONCLUSION AND FUTURE SCOPE

When applied to the APA-DDoS dataset, the hybrid machine learning algorithms exhibit impressive results for identifying Distributed Denial of Service (DDoS) attacks. A hybrid strategy that integrated Decision Tree with Random Forest, Gradient Boosting, and Naive Bayes techniques with AdaBoost and Support Vector Machines in all feasible combinations returned 100% accurate results. These findings demonstrate that ensemble techniques deliver enhanced classification precision and minimise false alarms while maintaining flexible attack detection capabilities. The detection process benefits most from key features, which include TCP flags and packet lengths, which are analysed through correlation heatmaps. The models demonstrated their correct identification of attack and regular traffic through flawless performance in the confusion matrices. While real-time DDoS detection in this study was supported by visual analytics tools such as bar plots, confusion matrix heatmaps, and funnel charts to validate the effectiveness of hybrid machine learning models, future work could focus on improving scalability to larger datasets, adapting models to evolving attack patterns, and integrating real-time deployment frameworks, thereby unlocking greater potential for robust cybersecurity in dynamic network environments.

Future studies might also build on this work by testing the suggested hybrid framework in live network traffic IoT scenarios to evaluate performance in varying conditions. By incorporating adaptive learning techniques, the model will be able to adapt to changing patterns of DDoS attacks. Further optimising resource utilisation in limited IoT devices can be achieved by investigating lightweight deployment on edge or fog nodes. Furthermore, incorporating explainable AI approaches could increase security analysts' accessibility, and combining them with federated learning or blockchain could improve data privacy and cooperative defence across dispersed IoT networks.

Table 4. Comparative analysis of different approaches for IoT DDoS detection.

Approach	Accuracy (Avg.)	Explain-Ability	Training Time	Resource Usage
Hybrid ML (This study)	99.99%	High	Low	Low
Deep Learning (CNN/LSTM) [22]	98–99%	Low	High	High
Traditional ML (Single Model) [23]	96–98%	Moderate	Moderate	Low–Moderate

LIST OF ABBREVIATIONS

SVM	=	Support Vector Machine
NN	=	Neural Network
DT	=	Decision Tree
RF	=	Random Forest
GB	=	Gradient Boost
NB	=	Naive Bayes
ML	=	Machine Learning
MLP	=	Multilayer Perceptron
K-NN	=	K-Nearest Neighbour
CNN	=	Convolutional Neural Network
LSTM	=	Long Short-Term Memory
IoT	=	Internet Of Things

AUTHORS' CONTRIBUTIONS

K.K.V. has contributed to the study concept, data collection, analysis, and manuscript writing. M.K. has contributed to data collection, writing, and proofreading.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The data will be made available on reasonable request by contacting the corresponding author [K.K.V.]

FUNDING

None.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this article.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

- [1] Nagpal B, Sharma P, Chauhan N, Panesar A. DDoS tools: classification, analysis and comparison. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom); 2015 Mar 11; New Delhi, India. p. 342-6. IEEE. <https://ieeexplore.ieee.org/document/7100270>.
- [2] Muragaa WH. A hybrid scheme for detecting and preventing single packet low-rate DDoS and flooding DDoS attacks in SDN. In: 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA); 2023 May 21; Tripoli, Libya. p. 707-12. IEEE. <https://doi.org/10.1109/MI-STA57575.2023.10169712>.
- [3] Toker O. Performance bounds for cyberattack detectors using multiple observations. In: SoutheastCon 2022; 2022 Mar 26; Mobile, AL, USA. p. 104-9. IEEE. <https://doi.org/10.1109/SoutheastCon48659.2022.9764036>.
- [4] Li L, Yang R. Optimal control for 2-D systems under malicious attacks. In: 2022 41st Chinese Control Conference (CCC); 2022 Jul 25; Hefei, China. p. 4245-50. IEEE. <https://doi.org/10.23919/CCC55666.2022.9902182>.
- [5] Pandey AK, Patel Y. IoT and ML based irrigation system using KNN algorithm. In: 2022 5th International Conference on Contemporary Computing and Informatics (IC3I); 2022 Dec 14; Uttar Pradesh, India. p. 779-84. IEEE. <https://doi.org/10.1109/IC3I56241.2022.10072613>.
- [6] Pandey AK, Adhvaryu R. ML accuracy assessment of DW transaction. In: 2022 5th International Conference on Contemporary Computing and Informatics (IC3I); 2022 Dec 14; Uttar Pradesh, India. p. 800-3. IEEE. <https://doi.org/10.1109/IC3I56241.2022.10073031>.
- [7] Hossain MA, Islam MS. Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: a promising solution for robust cybersecurity. Measurement. Sensors 2024; 32: 101037. <https://doi.org/10.1016/j.measen.2024.101037>.

- [8] Tomar A, Pant B, Tripathi V, Verma KK, Mishra S. Improving QoS of cloudlet scheduling via effective particle swarm model. In: Singh A, Gupta P, editors. Machine Learning, Advances in Computing, Renewable Energy and Communication. Singapore: Springer; 2021. p. 137-50. https://doi.org/10.1007/978-981-16-2354-7_13.
- [9] Sanmorino A, Marnisah L, Di Kesuma H. Detection of DDoS attacks using fine-tuned multi-layer perceptron models. Eng Technol Appl Sci Res 2024 ;14(5): 16444-9. <https://doi.org/10.48084/etasr.8362>.
- [10] Verma KK, Singh BM, Dixit A. A review of supervised and unsupervised machine learning techniques for suspicious behavior recognition in intelligent surveillance system. Int J Inf Technol 2022; 14(1): 397-410. <https://doi.org/10.1007/s41870-019-00364-0>.
- [11] Tay WY, Chin S, Chong YL. DDoS attack detection with machine learning. J Inform Web Eng 2024; 3(3):190-207. <https://doi.org/10.33093/jiwe.2024.3.3.12>.
- [12] Elubeyd H, Yiltas-Kaplan D. Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks. Appl Sci 2023;13(6):3828. <https://doi.org/10.3390/app13063828>
- [13] Roopesh M, Nishat N, Rasetti S, Rahaman MA. A review of machine learning and feature selection techniques for cybersecurity attack detection with a focus on DDoS attacks. Acad J Sci Technol Eng Math Educ 2024; 4(3): 178-94. https://www.researchgate.net/publication/384249930_A_REVIEW_OF_MACHINE_LEARNING_AND_FEATURE_SELECTION_TECHNIQUES_FOR_CYBERSECURITY_ATTACK_DETECTION_WITH_A_FOCUS_ON_DDOS_ATTACKS.
- [14] Kanthimathi S, Venkatraman S, Jayasankar KS, Jiljith TP, Jashwanth R. A Novel self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification. IEEE Access. 2024 Oct 11. <https://doi.org/10.48550/arXiv.2409.00810>.
- [15] Shaikh J, Butt YA, Naqvi HF. Effective intrusion detection system using deep learning for DDoS attacks. Asian Bull Big Data Manag 2024;4(1): 168-183. <https://doi.org/10.62019/abbdm.v4i1.113>.
- [16] Musa MO, Odokuma EE. A framework for the detection of distributed denial of service attacks on network logs using ML and DL classifiers. Sci Afr 2023; 22(3): 153-64. <https://doi.org/10.4314/sa.v22i3.14>.
- [17] Das P, Singh M, Verma KK. Blockchain-enabled deep learning approach to improve healthcare system. J Multimed Inf Syst 2024; 11(1): 9-16. <https://doi.org/10.33851/JMIS.2024.11.1.9>.
- [18] Zahid M, Bharati TS. Enhancing cybersecurity in IoT systems: a hybrid deep learning approach for real-time attack detection. Discov Internet Things 2025; 5(1): 73. <https://doi.org/10.1007/s43926-025-00156-y>.
- [19] Ain NU, Sardaraz M, Tahir M, Abo Elsoud MW, Alourani A. Securing IoT networks against DDoS attacks: a hybrid deep learning approach. Sensors 2025;25(5):1346. <https://doi.org/10.3390/s25051346>.
- [20] Mahdi ZS, Zaki RM, Alzubaidi L. Advanced hybrid techniques for cyberattack detection and defense in IoT networks. Secur Privacy. 2025 ;8(2): e471. <https://doi.org/10.1002/spy2.471>.
- [21] Sewaiwar P, Verma KK. Comparative study of various decision tree classification algorithms using WEKA. Int J Emerg Res Manag Technol. 2015 ; 4:2278-9359. <https://www.semanticscholar.org/paper/Comparative-Study-of-Variou-Decision-Tree-Using-Sewaiwar-Verma/7fd7b824fa44053551eb8f51a92a0bc590abe984>.
- [22] Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: current solutions and future challenges. IEEE Commun Surv Tutorials 2020; 22(3): 1686-721. <https://doi.org/10.1109/COMST.2020.2986444>.
- [23] Koroniotis N, Moustafa N, Sitnikova E, Turnbull B. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Gener Comput Syst 2019; 100:779-96. <https://doi.org/10.1016/j.future.2019.05.041>.