Received: August 24, 2024. Revised: October 22, 2024. 36

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Optimizing Intrusion Detection in Edge Computing Network: A Hybrid ML Approach with Recursive Feature Elimination

Amit Kumar[1]* Vivek Kumar[1] Abhay Pratap Singh Bhadauria[2]

[1]*Gurukula Kangri (Deemed to be University), Haridwar, U.K*
[2]*GLA University, Mathura, U.P*
* Corresponding author's Email: 19523002@gkv.ac.in

Abstract: As the prevalence of Internet of Things (IoT) devices increases, Cyber incidents are also increasing significantly. These Cyber incidents are mainly caused by various attacks, such as Distributed Denial of Service (DDoS), Denial of Service (DoS), intrusions, and web-based attacks. This type of attacks can severely impact valuable IoT system resources, compromise stored data, and lead to substantial financial losses if not adequately mitigated. Detecting these attacks within network traffic is complex and requires intelligent Intrusion Detection Systems (IDS). This paper proposes a Machine Learning (ML) based hybrid IDS model for edge computing networks. The feature selection process employs the 'Recursive Feature Elimination technique' (RFE) combined with 'Random Forest' (RF) to identify optimal features for attack detection. The Hybrid IDS model integrates 'Random Forest' (RF), 'Decision Tree' (DT), 'Extra Tree' (ET), and 'K-Nearest Neighbor' (KNN) algorithms. The Hybrid IDS model is evaluated on four datasets: 'CIC-IDS-2017', 'NSL-KDD', 'UNSW-NB15', and 'CSE-CIC-IDS-2018'. The results of the proposed model show maximum prediction accuracy of 99.92%, 99.89%, 99.50%, and 99.13%, and F1-score values obtained are 99.95%, 99.90%, 99.23%, and 99.13% on 'CIC-IDS-2017', 'NSL-KDD', 'UNSW-NB15', and 'CSE-CIC-IDS-2018' datasets, respectively. The experimental results clearly demonstrate that the proposed model performs better than the models reported in the existing studies.

Keywords: IoT devices, Edge computing, Feature selection, Cyber-attacks, Feature engineering.

1. Introduction

Recently IoT devices have been used to create smart environments including smart cities, homes, and vehicles. All these latest advancements cover a variety of services and enable significant advancements in connectivity, efficiency, and convenience. This marks a crucial milestone in the evolution of the Internet and digital transformation. Integrating IoT systems with intelligent computing has introduced many fascinating elements into our daily lives. However, IoT systems are vulnerable to a wide range of security threats, including malware, exploits, 'DoS (Denial of Service)', 'DDoS (Distributed Denial of Service)', 'Heartbleed', 'Infiltration', 'SQL injection', and 'Web-based attacks' [1]. Detecting these threats or attacks within network traffic is complex due to their evolving nature. Protecting against and preventing these increasingly sophisticated attacks with traditional security measures, such as web server security, firewalls, e-mail security, and antivirus programs, is no longer feasible. Such deadly attacks can disrupt critical services creating IoT and smart environments, potentially leading to data breaches as well as financial losses. An Intrusion Detection System (IDS) precautions the communication system by identifying imminent and potential threats or attacks [2].

Consequently, designing intelligent IDS systems to combat IoT attacks is crucial for researchers and developers [3]. In the IoT era, a vast amount of data is generated in real-time, making AI based systems a prime target [4]. Traditionally, this data is processed on cloud servers, but this has several drawbacks, including increased latency, higher connection costs, and privacy concerns. Edge computing (EC)

solutions have been proposed to overcome these challenges. In EC, devices are positioned near the IoT devices that generate the data and at the network's edge. This proximity enables computations to be performed nearer to the data sources, effectively addressing latency and bandwidth issues. However, security risks remain a significant concern in dynamic EC and IoT networks. Deploying intelligent machine learning (ML) systems or models to secure EC networks can mitigate these risks, offering a promising solution [5]. At the forefront of intrusion detection research, ML-based IDS are proving highly effective [2].

This study leverages ML algorithms including 'Random Forest (RF), Decision Tree (DT), Extra Tree (ET), and K-Nearest Neighbors (K-NN)' to build a robust hybrid intrusion detection system (IDS) for identifying critical attacks ("DoS, DDoS, Heartbleed, Intrusion, SQL Injection, and Web-based Attacks") in EC networks. The 'Recursive Feature Elimination with RF (RFE-RF)' method is applied to identify the most important and relevant features. The proposed hybrid IDS model is evaluated using four important datasets: 'CIC-IDS-2017', 'NSL-KDD', 'UNSW-NB15', and 'CSE-CIC-IDS-2018', all containing sophisticated cyber-attack network traces that have also been used in recent studies [6-7]. The proposed model aims to help administrators manage attacks in real-time or implement preventive measures and can be further enhanced to optimize detection processes in intrusion-based applications.

This paper is structured as follows. Section 2 examines the existing body of study. Section 3 presents a detailed methodology for intrusion detection, while Section 4 thoroughly evaluates the model. Section 5 presents the experimental results and does a comparison analysis with previous investigations. Section 6 summarizes the findings and discusses potential next directions.

2. Related work

Cyber-attacks, including DoS, DDoS, Heartbleed, Infiltration, SQL injection, and Web-based attacks, have surged with the widespread adoption of the Internet. Traditional IDS struggle to classify these attack patterns due to their hidden and sophisticated nature, allowing them to persist undetected within systems for prolonged periods. Consequently, these systems often need to identify attacks and their patterns [6] accurately. To enhance accuracy and detection rates (DR), ML-based techniques such as RF, DT, ET, and KNN have emerged, focusing on anomaly detection in network behavior or in IoT [7]. Various features and techniques have been investigated and utilized below to identify these attacks.

Saini et al. [7] proposed a system to detect Advanced Persistent Threat (APT) attacks using deep learning (DL) and ML models, including 'MLP (Multi-Layer Perceptron)', and 'CNN (Convolutional Neural Network)', and RF, DT. They used datasets such as 'CSE-CIC-IDS-2018, CIC-IDS-2017, NSL-KDD, and UNSW-NB15'. Their hybrid ensemble model, which consisted of RF and XGBoost classifiers, achieved a remarkably high prediction accuracy of 98.92%, 99.91%, 99.24%, and 97.11%, with false positive rates (FPR) of 0.52%, 0.12%, 0.62%, and 5.29%. The effective features are achieved using, Information Gain (IG), Pearson correlation, and SHAP (SHapleyAdditive exPlanations) approaches. The proposed model failed to achieve sufficient accuracy on the CIC-IDS-2018, NSL-KDD, and UNSW-NB15 datasets, indicating its limitations in detecting attacks within these datasets. Particularly, the FPR was exceptionally high on the UNSW-NB15 dataset, which is our main concern in the studies to mitigate FPR.

Tripathi et al. [8] proposed a new strategy for improving feature selection in ML systems for network intrusion detection. Using the CICIDS-2017 dataset, their approach optimizes feature selection and reduction by focusing on high-impact characteristics. The approach reduced irrelevant attributes by 51%, increasing the tuned RF detection accuracy with 40 essential features to 99.9% with a precision of 99.80%, recall at 99.89%, and f1-score of 99.85%. However, forty features are selected using the CHI-REV based approach. These features are reported to be relevant for improving model performance. However, practical feature selection approaches are needed to improve model performance further to obtain essential features. However, FPR has not been utilized in their study.

Mokbal et al. [9] presented an IDS framework that combines the extreme gradient boosting (XGBoost) algorithm with an integrated feature selection method. Their framework underwent rigorous evaluation with extensive test data, including binary and multi-classification scenarios. They selected fifty important features using an embedded feature selection approach. Authors achieved good performance in various metrics, including overall accuracy of 99.86%, precision of 99.69%, detection rate (DR) of 99.75%, specificity of 99.69%, F-score of 99.72%, false negative rate (FNR) of 0.17%, FPR of 0.2%, error rate of 0.14%, and area under the curve (AUC) of 99.72%. These fifty features have proven sufficient to improve the model's performance. However, the precision and

DR are relatively low, which is very important for the classification-based model.

Manokaran et al. [10] enhanced anomaly detection performance by integrating optimized ensemble learning algorithms, including Adaptive Boosting (AdaBoost), RF, XGBoost, and Light Gradient Boosting Machine (LGBM), with a novel hybrid feature selection method. They developed an Improved Particle Swarm Optimization (IPSO) algorithm, combining elimination and opposition-based learning, hybridized with the Chi-square method (Chi-IPSO). The model was evaluated on the UNSW-NB-15 dataset and reached 94.58% accuracy using network traffic features. Moreover, the model achieved 99.70% accuracy using CIC-IDS-2017 dataset containing the several features of statistical network traffic. However, the proposed model failed to detect attacks efficiently which utilizes the UNSW-NB15 and 'CIC-IDS-2017' datasets due to the complex selection of the features.

Arif Faizin et al. [11] proposed an IDS integrating mutual information (MI) with thresholding feature selection and the XGBoost classification algorithm. By measuring the dependency between input and target features, they applied thresholding to optimize the number of features for classification. The UNSW-NB15 dataset has been used to select the best feature selection method and thresholding value. The accuracy of the proposed model is 87.63% which is low compare to the existing studies.

OYELAKIN et al. [12] conducted a study using the CIC-IDS-2017 intrusion dataset to build a Cyber threat detection model. They utilized the XgBoost feature importance approach for selecting thirty-four features. They achieved good accuracy in identifying cyber intrusions using these features. The model substantiated impressive performance with an average accuracy of 98%, recall of 0.98, F1-score of 0.98, precision of 0.98, and an AUC-ROC score of 0.99. However, based on the relative results and the selected features, the proposed model is not sufficient to detect attacks on the CIC-IDS-2017 dataset.

Hasanah et al. [13] proposed a comprehensive intrusion detection system model that consists of three stages: data preprocessing, feature selection using ANOVA F-value with cross-validation, and classification using a weighted voting classifier. This classifier combines RF, kernel neural network, and logistic regression. Furthermore, the proposed technique has achieved an average accuracy of 95.51% and precision of 98.66%.

According to related work, many ML based approaches have been recognised in the past few years, but they still suffer several shortcomings. Moreover, they failed to find the optimal set of features to detect attacks, and the selection of irrelevant features significantly affected the classification performance. We understand that optimal feature selection will enhance the performance of IDS, which is the primary concern of our work. Therefore, the RFE-RF technique efficiently selects the optimal set of features for our proposed model, resulting in improved performance. Moreover, for critical distributed EC networks, the performance of a single classifier is not a reasonable approach Therefore, we utilized an amalgamation of ML Classifiers designed to provide a significant performance boost through a soft voting method. This method reduces variance and bias, leading to more effective model training and improved performance.

3. Methodology

The process for managing all datasets and hybrid models intended for attack detection and classification is illustrated in Fig. 1. Interestingly, our novel strategy—which uses the hybrid model with soft voting—creates a new standard and greatly improves the performance of the current models in every scenario. This performance improvement is most noticeable in the pre-processing stage of data preparation, followed by efficient feature optimization utilizing the RFE-RF technique—essential for the high accuracy, detection rate and low FPR. Classifiers are then assessed to build the best possible model. Four datasets, including historical and modern ones, will be used to evaluate the effectiveness of the suggested model: CIC-IDS-2017, NSL-KDD, CSE-CIC-IDS-2018, and UNSW-NB15 [14-17].

3.1 Datasets description

The NSL KDD, UNSW-NB15, CIC-IDS-2017, and CIC-IDS-2018 datasets capture intrusion incidents in edge computing and IoT networks. These datasets highlight unauthorized and potentially malicious actions that threaten the security and integrity of edge and IoT devices and data. Such intrusions can lead to significant consequences, including data breaches, service interruptions, and privacy violations, underscoring the critical need for robust Cybersecurity measures in these environments.

3.1.1. NSL-KDD

The NSL-KDD dataset, a precocious version of the KDD Cup 1999 dataset, is valued for evaluating IDS. The NSL-KDD dataset features diverse network

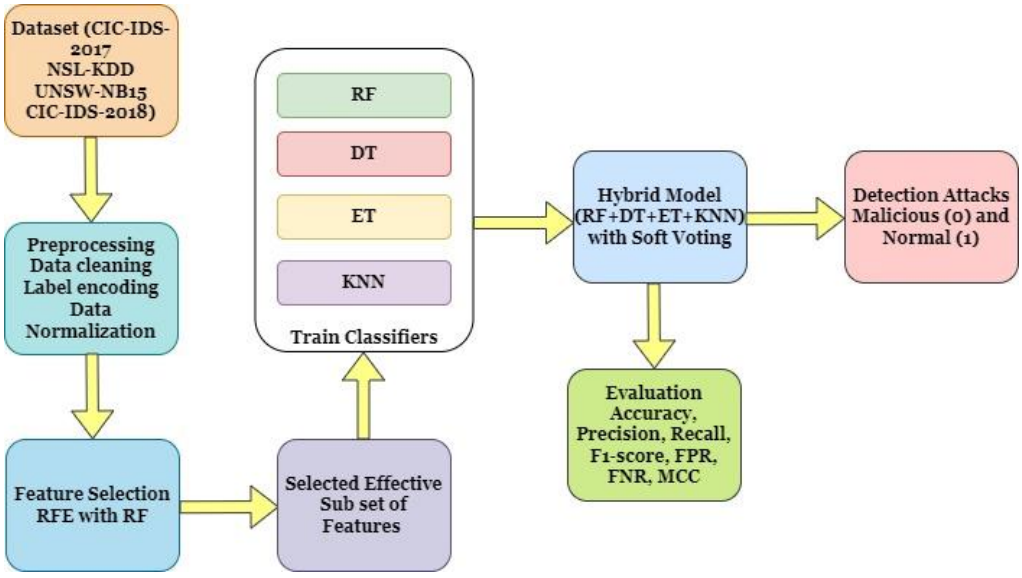

Figure. 1 Proposed Hybrid IDS Model Architecture

traffic data divided into regular and attack classes. The dataset comprises 67,342 benign and 58,630 malicious records, totalling 125,973 records with 41 features. The attacks are categorized into four primary types: DoS (45,927 records), Remote to Local (R2L, 955 records), User to Root (U2R, 52 records), and Probe (11,656 records), offering a comprehensive evaluation resource for IDS [14].

3.1.2. UNSW-NB15

The 'UNSW-NB15' dataset is a comprehensive synthetic network traffic dataset created by the 'University of New South Wales (UNSW)' designed for evaluating IDSs. It includes a varied range of attack scenarios categorized into nine types: 'Backdoors (1,746 records), DoS (12,264), Shellcode (1,133), Exploits (33,393), Fuzzers (18,184), Analysis (2,000), Generic (40,000), Reconnaissance (10,491), and Worms (130)', alongside 56,000 records of normal traffic. The dataset included 49 features using Argus and Bro-IDS tools, which provided a comprehensive contribution to the evaluation of IDS [15]. The dataset contains 56,000 benign and 119,341 malicious records, totalling 175,341 records. These are used to detect malicious traffic in network traffic.

3.1.3. CIC-IDS-2017

The CIC-IDS2017 dataset is a valuable resource for evaluating network traffic and recent attack patterns, comprising eight CSV files: one with normal flows (2,273,097 records) and seven with malicious flows. The dataset contains total 2,830,743 records and 80 features, providing comprehensive coverage of network scenarios and attacks [16]. The malicious categories include DoS Hulk (231,073 records), PortScan (158,930), DDoS (128,027), FTP-Patator (7,938), SSH-Patator (5,897), DoS Slowloris (5,796), DoS Slowhttptest (5,499), Bot (1,966), Web Attack Brute Force (1,507), Web Attack XSS (652), Infiltration (36), Web Attack SQL Injection (21), and Heartbleed (11).

3.1.4. CSE-CIC-IDS-2018

The CSE-CIC-IDS2018 dataset, developed by CIC, aims to advance network security research by covering various Cyber-attack scenarios with 80 plus features. It includes aprox millions records of benign traffic and multiple attack types. This study collected attacks types: DDOS Attack-HOIC (68,692 records), DoS Attack-Hulk (45,983), Bot (28,705), FTP-Bruteforce (19,469), SSH-Bruteforce (18,875), DoS Attack-SlowHTTPTest (14,154), Infiltration (6,864), DoS Attack-GoldenEye (4,157), DoS Attack-SlowLoris (1,139), DDOS Attack-LOIC-UDP (181), Brute Force-Web (25), Brute Force-XSS (8), and SQL Injection (5). The dataset provides a comprehensive overview of network security advancements [17]. Table 1 shows the attack statistics including benign/normal attacks for CIC-IDS-2017, NSL-KDD, and UNSW-NB15.

Table 1. Normal and malicious flows/records in datasets

Attacks Types	CIC-IDS-2017	NSL-KDD	UNSW-NB15	CSE-CIC-IDS-2018
Benign	2,271,320	67,342	56,000	10,00 00
Maliciou s/Attacks	5, 565,56	58,630	1,19,34 1	10,00 00
Total	28,27,87 6	1,25,97 32	1,75,34 1	20,00 00

3.2 Pre-processing

Data pre-processing transforms raw or noisy data into a clean dataset, ensuring accuracy and usability through error removal and formatting. Therefore, three kinds of processes are included in data pre-processing: Data cleaning, Label encoding, and Data Normalization, which are briefly explained below.

3.2.1. Data cleaning

The CIC-IDS-2017 dataset, containing 2,830,743 records, was cleaned, and 2,867 records with missing and infinite values were removed. Table 1 details the attack statistics for 'CIC-IDS-2017, NSL-KDD' (which has no duplicate values), and UNSW-NB15 (which includes both normal and malicious flows and has no duplicates). These datasets offer comprehensive resources for evaluating network traffic and attack scenarios. The CSE-CIC-IDS2018 dataset, an extensive collection of CSV files with millions of records, required substantial time and computational resources, leading to stratified random sampling to select 0.10 fractions from each file. Experience the power of our approach, where every dataset is carefully allocated: 80% for training to build robust models and 20% for rigorous testing to ensure reliability.

3.2.2. Label encoding

Label encoding is an ML technique that converts categorical data into a numerical format by assigning each category a unique integer. The dataset includes both numerical and non-numerical label values. The machine learning process is based on numerical calculations. This requires the transformation of non-numerical objects into numerical objects. This transformation assigns 0 ('malicious') and 1 ('normal') to the eight attributes in the labels - 'normal, brute force, DoS, DDoS, intrusion, botnet, portscan, and web attack', ensuring clear and accurate classification.

3.2.3. Data normalization

Data normalization scales data to a standard range, typically from 0 to 1. This enhancement significantly boosts algorithm performance and convergence by mitigating biases arising from variations in feature magnitudes.

$$X_{scaled} = \frac{y - min\,(y)}{max(y) - min\,(y)} \quad (1)$$

Where $max\,(y)$ = maximum, $min(y)$ = minimum records of the feature x. The high variance values given by Eq. (1) are normalized using the min-max scaling technique.

3.2.4. Feature selection

Feature selection is critical for identifying the relevant features and minimizing data dimensions. This work employed the RFE method with an RF classifier to pick the right features. This method allows to selection of effective features that effectively reduce the data dimensions while maintaining or improving the model accuracy. Algorithm 1 shows the RFE with the RF process. Fig. 2, 3, 4, and 5 display the significant features selected using 'CIC-IDS-2017, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS-2018', respectively.

Algorithm 1: RFE with RF Process

Input: N_f: All Sub set of Features
P_f: Group optimal Features
Output: P_f

1. **For** *i* in range 1 to N_f:
2. *Sel←RFE(RandomForestClassifier(n_estimators←50,random_state←0), n_features_to_select←features)*
3. *Sel.fit (x_train, y_train)*
4. *X_train$_{rfe}$ ←Sel.transform(x_train)*
5. *X_test$_{rfe}$ ←Sel. transform(x_test)*
6. *Print ('Selected Feature: ', i)*
7. *Clasif←RandomForestClassifier(n_estimators←50, random_state←0, jobs←-1)*
8. *Clasif.fit (X_train$_{rfe}$, y_train)*
9. *Features ←x_train. columns [Sel.getsupport()]*
10. *Return P_f*
11. **end**

The algorithm1 proposes a feature selection procedure that uses RFE with an RF classifier to identify a subset of insightful features from the dataset. The algorithm iterates over each subset of features (N_f), starting from 1 up to the total number of features (N_f). For each subset, RFE is initialized with an RF classifier. This is done with 50 estimators (trees) and a fixed random position for consistency. *n_features_to_select←features* ensure that the algorithm selects a specific number of features to keep. The RFE model is fitted to the training data (*x_train, y_train*). This step identifies which features are necessary to predict the output based on the RF performance. The fitted RFE model transforms both the training (*X_trainrfe*) and testing data (*X_testrfe* variables) by reducing the dataset to only the selected features. For each iteration *i*, the algorithm displays or prints which subset of features is currently being

evaluated. A new RF classifier with 50 estimators is created and is enabled by parallel processing (*jobs←-1*). This classifier is trained using the reduced training set (*X_trainrfe*) with only the selected features. The algorithm obtains the names of the selected features by applying the *Sel.getsupport()* method on the original feature set (*x_train.columns*). After completing the iterations, the optimal subset of features (P_f) is returned as the final output.

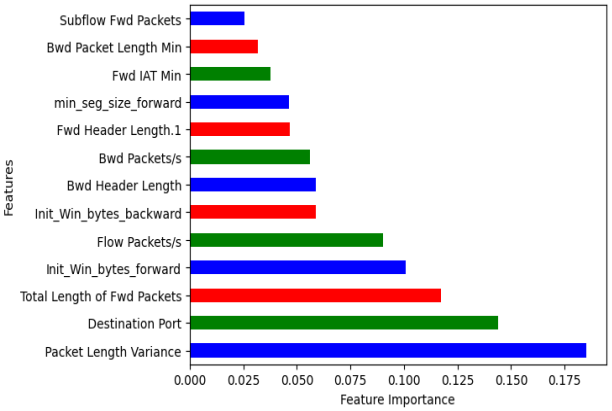

Figure. 2 List of optimal features using CIC-IDS-2017

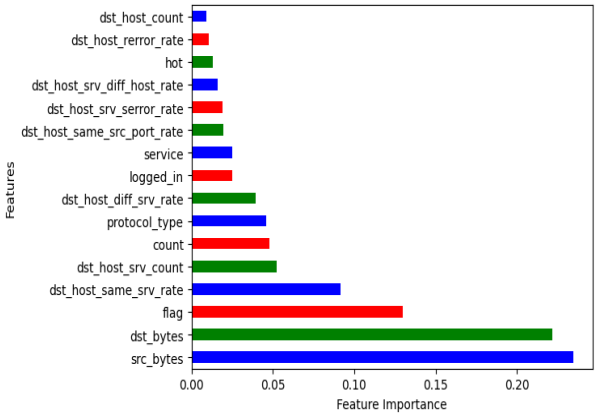

Figure. 3 List of optimal features using NSL-KDD

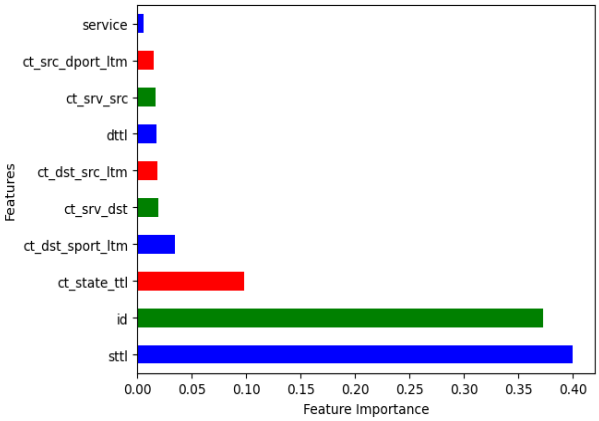

Figure. 4 List of optimal features using UNSW-NB15

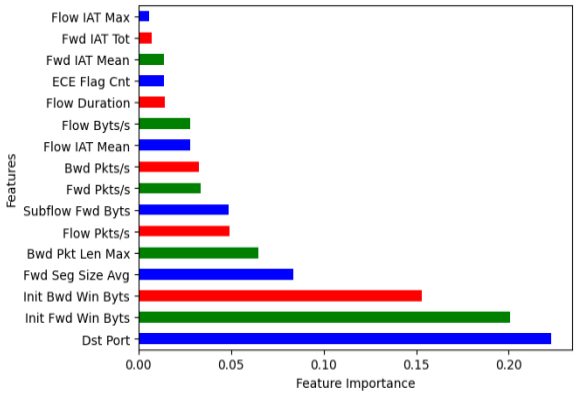

Figure. 5 List of optimal features using CIC-IDS-2018

3.3 Proposed model

This section emphasizes the effectiveness of ensemble learning techniques in developing the proposed hybrid model for attack detection. Ensemble learning, a comprehensive ML strategy, enhances predictive accuracy by combining multiple model predictions. It encompasses three types: bagging, boosting, and stacking/voting. Bagging applies one algorithm to various training subsets with replacement but its reliance on random selection can affect classification performance. Boosting trains weak learners to improve model accuracy, though its interdependent inputs make parallelization challenging [9]. Both bagging and boosting utilize homogeneous classifiers and perform well on small datasets. In contrast, stacking/voting is more effective with large datasets and diverse models, enhancing prediction accuracy. This study adopts the soft voting approach, which assigns probability values to data items for class assessment, yielding better results by prioritizing confident votes [9]. The proposed hybrid IDS model integrates RF, DT, ET, and K-NN classifiers with soft voting, as depicted in Figure 1, which showcases a thorough model development process.

4. Evaluation of model

Fig. 6 shows a typical confusion matrix with four elements (TP, TN, FP, and FN). Different performance indicators were utilized to evaluate the model, which is presented in Eqs. (2)-(9).

Understanding True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN) are crucial for accurately identifying attacks and normal activities. TP indicates correctly identified attacks, while TN indicates accurately classified normal activities. Conversely, FP represents normal activities mistakenly classified as attacks, and FN denotes attacks incorrectly identified as normal.

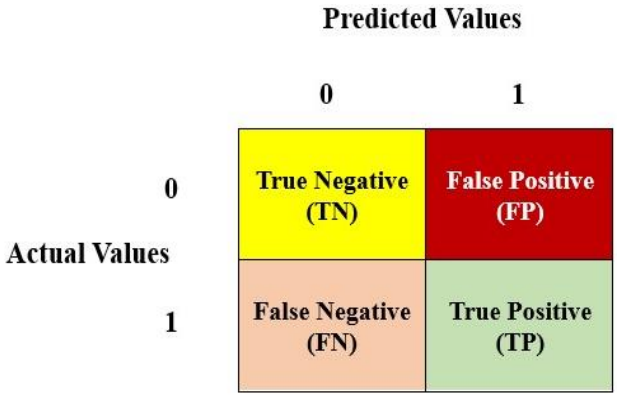

Figure. 6 Confusion matrix

Accuracy

$$Accuracy = \frac{Tp+Tn}{Tp+Fp+Tn+Fn} \quad (2)$$

Recall (RC) or DR

$$RC = \frac{Tp}{Tp+Fn} \quad (3)$$

Precision (PR)

$$PR = \frac{Tp}{Tp+Fp} \quad (4)$$

FPR

$$FPR = \frac{Fp}{Fp+Tn} \quad (5)$$

F1-Score

$$F1\text{-}score = \frac{2*PR*RC}{PR+RC} \quad (7)$$

FNR

$$FNR = \frac{Fn}{Tp+Fn} \quad (8)$$

4.7 MCC (Matthew's correlation coefficient)

The MCC is a powerful metric that evaluates the accuracy of binary classifications. It provides a clear and concise measurement on a scale from -1 to +1. This metric is calculated using the formula [10]:

$$MCC = \frac{Tp*Tn - Fp*Fn}{\sqrt{((Tp+Fp)(Tp+Fn)(Tn+Fp)(Tn+Fn))}} \quad (9)$$

5. Experimental results & discussion

This proposed work utilizes a new ML-based hybrid model to distinguish between normal and malignant attack classes. Using RFE with RF for optimal feature selection, this research focuses on improving detection accuracy, recall, precision, and high FPR. The hybrid model was carefully evaluated on benchmark datasets, including CIC-IDS-2017, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS-2018, chosen for their widespread use in Cybersecurity and the representation of diverse attack scenarios. Our novel approach employs ML classifiers, including RF, DT, ET, and KNN, in a unique ensemble-based hybrid model.

In Table 2, presented the individual performance of models RF, DT, ET, and KNN alongside our hybrid model using the CIC-IDS-2017 dataset, and the accuracies achieved are 99.92%, 99.92%, 99.89%, 99.90%, and 99.34%, respectively, demonstrating the robustness and reliability of our hybrid model.

Table 3 shows the results which utilizes the NSL-KDD dataset; for the hybrid model, RF, DT, ET, and KNN, the accuracies achieved are 99.89%, 99.91%, 99.82%, 99.83%, and 99.56%. Table 4 also provides insights utilizing the UNSW-NB15 dataset results, the accuracies achieved for the hybrid model, RF, DT, ET, and KNN being 99.50%, 99.32%, 99.38%, 99.31%, and 98.77%. Additionally, Table 5 presents the accuracies and several other evaluation indicators achieved which utilizes the CIC-IDS2018 dataset.

Table 6 provides a comprehensive summary of the results, indicating that the suggested hybrid model delivers superior performance across multiple key measures such as accuracy, precision, recall, F1-score, FNR, and MCC.

Table 2. Evaluation results for CIC-IDS-2017

Models	Accuracy (in %)	PR (in %)	RC (in %)	F1-Score (in %)	FPR (in %)
RF	99.92	99.97	99.93	99.95	0.001
DT	99.89	99.94	99.92	99.93	0.002
ET	99.90	99.94	99.93	99.94	0.002
KNN	99.34	99.72	99.46	99.59	0.011
Hybrid Model	**99.92**	**99.97**	**99.93**	**99.95**	**0.001**

Table 3. Evaluation results for NSL-KDD

Models	Accuracy (in %)	PR (in %)	RC (in %)	F1-Score (in %)	FPR (in %)
RF	99.91	99.91	99.93	99.92	0.001
DT	99.82	99.88	99.79	99.84	0.001
ET	99.83	99.85	99.84	99.84	0.001
KNN	99.56	99.70	99.48	99.59	0.003
Hybrid Model	**99.89**	**99.91**	**99.88**	**99.90**	**0.001**

Table 4. Evaluation results for UNSW-NB15

Models	Accuracy (in %)	PR (in %)	RC (in %)	F1-Score (in %)	FPR (in %)
RF	99.32	99.23	98.63	98.93	0.003
DT	99.38	98.87	99.22	99.04	0.005
ET	99.31	98.95	98.94	98.95	0.004
KNN	98.77	97.95	98.26	98.11	0.009
Hybrid Model	**99.50**	**99.27**	**99.18**	**99.23**	**0.003**

Table 5. Evaluation results for CSE-CIC-IDS-2018

Models	Accuracy (in %)	PR (in %)	RC (in %)	F1-Score (in %)	FPR (in %)
RF	99.20	99.94	98.47	99.20	0.0006
DT	99.18	99.95	98.40	99.17	0.0004
ET	99.05	99.61	98.50	99.05	0.003
KNN	99.10	99.73	98.47	99.10	0.002
Hybrid Model	**99.13**	**99.73**	**98.53**	**99.13**	**0.002**

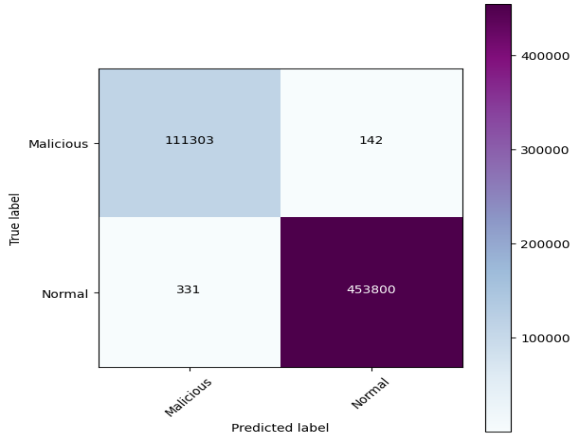

Figure. 7 Confusion matrix of Hybrid model using CIC-IDS-2017

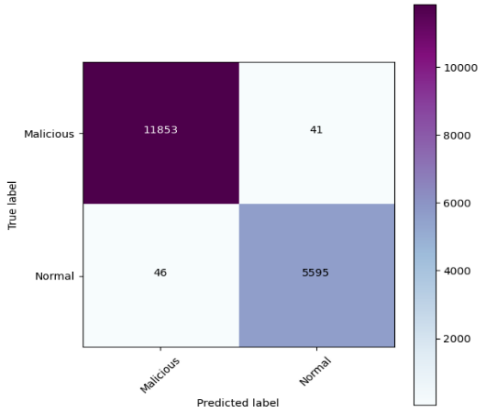

Figure. 9 Hybrid model confusion matrix based on UNSW-NB15

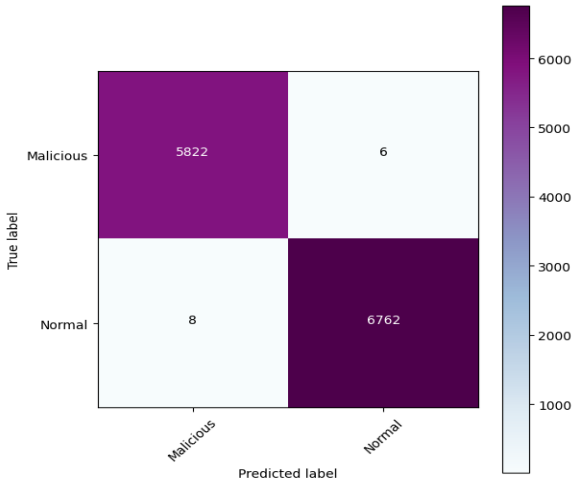

Figure. 8 Hybrid model confusion matrix based on NSL-KDD

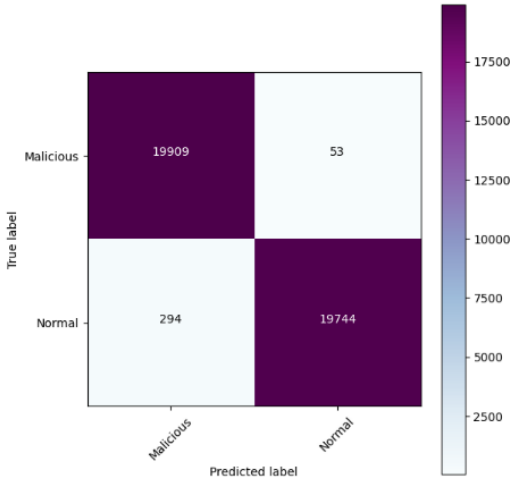

Figure. 10 Confusion matrix of Hybrid model using CSE-CIC-IDS2018

The proposed hybrid model achieved prediction accuracies of 99.92%, 99.89%, 99.50%, and 99.13%, high average precision values of 99.97%, 99.91%, 99.27%, and 99.73%, and recall values of 99.93%, 99.88%, 99.18%, and 98.53% using CIC-IDS-2017, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS2018 dataset and compared existing techniques such as Hybrid-IDS-Model (RF+XGBoost) [7], Chi-rev [8], XgBoost [9], Chi-IPSO-RF [10], MI with thresholding feature selection with XGBoost classification algorithm [11], XgBoost [12], ANOVA F-value CV with Weight based voting classifier [13], and PACENIDS [18]. Furthermore, the proposed model validated low FPR of 0.001%, 0.001%, 0.003%, and 0.002%, high F1-scores of 99.95%, 99.90%, 99.23%, and 99.13%, low FNRs of 0.0007%, 0.001%, 0.008%, and 0.014% compared existing techniques Hybrid-IDS-Model (RF+XGBoost) [7], XgBoost [9], and PACENIDS [18]. A Chi-IPSO-RF model was also established by [10] for intrusion detection, with MCC values of 63.38% on UNSW-NB15 and 99.49% on CIC-IDS-2017 datasets. In comparison, the proposed hybrid model shows good MCC values of 99.73% on CIC-IDS-2017, 99.77% on CIC-IDS-2018, 98.86% on UNSW-NB-15, and 98.27% on the CIC-IDS-2018 dataset. Fig. 7-10 visually represents the confusion matrices, illustrating our model's effectiveness with different datasets.

Table 6. Comparison results of proposed Hybrid model

Authors	**Techniques applied**	**Dataset used**	**Accuracy**	**PR**	**TPR/RC/ Sensitivity/DR**	**FPR**	**F1-Score**	**FNR**	**MCC**
[7]	Hybrid-IDS-Model (RF+XGBoost)	CSE-CIC-IDS2018	98.92%	99.47%	98.35%	0.52%	98.90%	1.65%	-
		CIC-IDS2017	99.91%	99.88%	99.95%	0.12%	99.91%	0.05%	-
		NSL-KDD	99.24%	99.28%	99.09%	0.62%	99.18%	0.91%	-
		UNSW-NB15	97.11%	95.89%	97.44%	5.29%	97.44%	0.96%	-
[8]	Chi-rev, RF	CIC-IDS-2017	99.90%	99.80%	99.89%	-	99.85%	-	-
[9]	XgBoost	CIC-IDS-2017	99.86%	99.69%	-	0.2%	99.72%	0.17%	-
[10]	Chi-IPSO-RF	UNSW-NB15	94.58%	95.90%	98.55%	-	98.59%	-	63.38%
		CIC-IDS-2017	99.70%	99.64	99.32%	-	99.55%	-	99.49%
[11]	MI with thresholding feature selection and XGBoost classification algorithm	CICIDS2017	99.89%	99.75%	99.60%	-	99.68%	-	-
		NSL-KDD	80.51%	68.06%	96.73%	-	79.90%	-	-
		UNSW-NB-15	87.63%	96.35%	83.66%	-	89.56%	-	-
[12]	XgBoost	CIC-IDS-2017	98%	98%	98%	-	98%	-	-
[13]	ANOVA F-value CV and Weight based voting classifier	UNSW-NB15	95.51%	98.66%	96.09%	-	96.73%	-	-
[18]	PACENIDS	NSL-KDD	96.59%	94.69%	99.29%	6.62%	96.93%	-	-
Proposed Work Hybrid Model (RF+DT+ET+KNN), Feature Selection RFE with RF		**CIC-IDS-2017**	**99.92%**	**99.97 %**	**99.93%**	**0.001 %**	**99.95 %**	**0.0007 %**	**99.73 %**
		NSL-KDD	**99.89%**	**99.91 %**	**99.88%**	**0.001 %**	**99.90 %**	**0.001%**	**99.77 %**
		UNSW-NB15	**99.50%**	**99.27 %**	**99.18%**	**0.003 %**	**99.23 %**	**0.008%**	**98.86 %**
		CIC-IDS-2018	**99.13%**	**99.73 %**	**98.53%**	**0.002 %**	**99.13 %**	**0.014%**	**98.27 %**

5.1 Comparative analysis

This section mainly deals with the results obtained utilizing several ML-based classifiers, and other existing studies are compared. The simulation results retrieved by the proposed approach are portrayed in Table 6. It is clearly stated that the proposed hybrid model achieves better accuracy than all other existing studies. Improvements in results were also noticed in terms of several evaluation metrics. Furthermore, the proposed study computed the FPR and FNR, while some existing studies have not considered or obtained high FPR and FNR. FPR and FNR are two important evaluation indicators in any AI-based model. High FPR and FNR leads to misclassification results in any detection model. Therefore, our primary concern in this research work is to mitigate both FPR and FNR. The FPR and FNR are very low when compared to the existing studies [7, 9, 18]. We also utilized an optimal subset of features using the REF-RF-based method which enhances the mechanism of the proposed IDS model.

6. Conclusion

This study proposes a hybrid model using RF, DT, ET, and K-NN algorithms to classify attacks. Many IDS using ML based techniques and faces issues such as insufficient features, low detection accuracy, high FNR, and high FPR. Therefore, in this study features were obtained using the RFE-RF technique for optimal feature selection. The model was rigorously tested on four diverse datasets: CIC-IDS-2017, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS-2017. The Hybrid IDS model delivered impressive results across four datasets with prediction accuracies of 99.92%, 99.89%, 99.50%, and 99.13%. It achieved high average precision values of 99.97%, 99.91%, 99.27%, and 99.73%, and recall or DR values of 99.93%, 99.88%, 99.18%, and 98.53%. The model also attested low FPR of 0.001%, 0.001%, 0.003%, and 0.002%, and high F1-scores of 99.95%, 99.90%, 99.23%, and 99.13%. Additionally, it showed low FNR of 0.0007%, 0.001%, 0.008%, and 0.014%, with perfect MCC of 99.73%, 99.77%, 98.86%, and 98.27%. These metrics underscore the model's effectiveness and reliability in detecting attacks with high accuracy and minimal errors. These results highlighted our Hybrid IDS model's superiority over existing solutions, demonstrating its effectiveness in enhancing the security of edge computing against advanced Cyber-attacks in real-time.

Conflicts of Interest

Authors declare no conflict of interest.

Author Contributions

Conceptualization AK, VK; methodology AK, VK; software AK, and VK; analysis AM, and, writing original draft preparation AK and VK; validation and reviewing the manuscript by APS Bhadauria.

References

[1] M. A. Alaketu, A. Oguntimilehin, K. A. Olatunji, O. B. Abiola, B. Badeji-Ajisafe, C. O. Akinduyite, and T. Okebule, “Comparative analysis of intrusion detection models using big data analytics and machine learning techniques”, *International Arab Journal Information Technology*, Vol. 21, No. 2, pp. 326-337, 2024.

[2] M. Mulyanto, J. S. Leu, M. Faisal, and W. Yunanto, "Weight embedding autoencoder as feature representation learning in an intrusion detection system”, *Computers and Electrical Engineering*, Vol. 111, pp. 108949, 2023.

[3] E. M. Faisal, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey”, *Journal of Cloud Computing*, Vol. 1, pp. 1-20, 2018.

[4] Z. Chang, S. Liu, X. Xiong, et al., "A survey of recent advances in edge-computing-powered artificial intelligence of things”, *IEEE Internet of Things Journal*, Vol. 8, No. 18, pp. 13849-13875, 2021.

[5] X. Wang, Y. Han, C. Wang, et al., "In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning”, *IEEE Network*, Vol. 33, No. 5, pp. 156-165, 2019.

[6] W. Y. B. Lim, N. C. Luong, D. T. Hoang, et al., "Federated learning in mobile edge networks: A comprehensive survey”, *IEEE Comm. Surveys & Tutorials*, Vol. 22, No. 3, pp. 2031-2063, 2020.

[7] N. Saini, B. Kasaragod V. Bhat, K. Prakasha, and A. K. Das, "A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection”, *Concurrency and Computation: Practice and Experience*, Vol. 35, No. 28, pp. e7865, 2023.

[8] G. Tripathi, V. K. Singh, V. Sharma, and M. V. Vinodbhai, "Weighted feature selection for machine learning based accurate intrusion detection in communication networks”, *IEEE Access*, Vol. 12, pp. 20973-20982, 2024.

[9] F. M. M. Mokbal, D. Wang, M. Osman, P. Yang, and M. Alsamhi, "An efficient intrusion detection framework based on embedding feature selection and ensemble learning technique", *International Arab Journal Information Technology*, Vol. 19, No. 2, pp. 237-248, 2022.

[10] J. Manokaran, V. Gurusamy, O. Khalaf, S. Algburi, and H. Hamam, "An efficient anomaly detection system in IoT edge using Chi Square-Improved Particle Swarm Optimization feature selection with ensemble classifiers", *International Journal of Computing and Digital Systems*, Vol. 16, No. 1, pp. 1-14, 2024.

[11] M. A. Faizin, D. T. Kurniasari, N. Elqolby, M. Aidie, and T. Ahmad, "Optimizing feature selection method in intrusion detection system using thresholding", *International Journal of Intelligent Engineering and Systems*, Vol. 17, No. 3, 2024, doi: 10.22266/ijies2024.0630.18.

[12] A. M. Oyelakin, "A learning approach for the identification of network intrusions based on ensemble XGBoost classifier", *Indonesian Journal of Data and Science*, Vol. 4, No. 3, pp. 190-197, 2023.

[13] M. Hasanah, R. A. Putri, M. Aidie, and R. Putra, "Analysis of weight-based voting classifier for intrusion detection system", *International Journal of Intelligent Engineering and Systems*, Vol. 17, No. 2, 2024, doi: 10.22266/ijies2024.0430.17.

[14] "NSL-KDD dataset", [Online]. Available: *https://www.unb.ca/cic/datasets/nsl.html.*

[15] UNSW Canberra at ADFA, "The UNSW-NB15 dataset", [Online]. Available: *https://research.unsw.edu.au/projects/unsw-nb15-dataset.*

[16] "CICIDS2017 Dataset." [Online]. Available: *https://www.unb.ca/cic/datasets/ids-2017.html*

[17] Canadian Institute for Cyber Security (CIC), "CSE-CIC-IDS 2018 on AWS", [Online]. Available: *https://www.unb.ca/cic/datasets/ids-2018.html.*

[18] N. Girubagari, T. N. Ravi, "Parallel ABILSTM and CBIGRU Ensemble Network Intrusion Detection System", *International Journal of Intelligent Engineering and Systems*, Vol.17, No.1, 2024, doi: 10.22266/ijies2024.0229.10.