Hindawi
Wireless Communications and Mobile Computing
Volume 2024, Article ID 5522431, 15 pages
https://doi.org/10.1155/2024/5522431

Research Article

A Novel Hybrid Feature Selection with Cascaded LSTM: Enhancing Security in IoT Networks

Karthic Sundaram,[1] **Yuvaraj Natarajan**,[1] **Anitha Perumalsamy**,[2] **and Ahmed Abdi Yusuf Ali**[3]

[1]*Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore 641407, India*
[2]*Department of Computer Science and Engineering, Coimbatore Institute of Technology, Coimbatore 641014, India*
[3]*Department of Electrical Engineering, University of Johannesburg, Johannesburg 2092, South Africa*

Correspondence should be addressed to Karthic Sundaram; karthic.s@kpriet.ac.in

Received 9 November 2023; Revised 31 January 2024; Accepted 27 February 2024; Published 13 March 2024

Academic Editor: Sandhya Aneja

The rapid growth of the Internet of Things (IoT) has created a situation where a huge amount of sensitive data is constantly being created and sent through many devices, making data security a top priority. In the complex network of IoT, detecting intrusions becomes a key part of strengthening security. Since IoT environments can be easily affected by a wide range of cyber threats, intrusion detection systems (IDS) are crucial for quickly finding and dealing with potential intrusions as they happen. IDS datasets can have a wide range of features, from just a few to several hundreds or even thousands. Managing such large datasets is a big challenge, requiring a lot of computer power and leading to long processing times. To build an efficient IDS, this article introduces a combined feature selection strategy using recursive feature elimination and information gain. Then, a cascaded long–short-term memory is used to improve attack classifications. This method achieved an accuracy of 98.96% and 99.30% on the NSL-KDD and UNSW-NB15 datasets, respectively, for performing binary classification. This research provides a practical strategy for improving the effectiveness and accuracy of intrusion detection in IoT networks.

1. Introduction

The fast growth of the Internet has dramatically changed how people communicate, access information, and use technology. It has smoothly blended into modern society, impacting many areas of our lives. However, this growth and increased connectivity have also led to a significant rise in cyber-attacks [1]. This widespread interconnectivity offers cybercriminals many potential targets to exploit. In the area of Internet of Things (IoT) environments, intrusion detection systems (IDS) play a vital role by proactively finding and responding to cybersecurity threats. This helps improve the overall resilience and security of IoT ecosystems, effectively protecting critical infrastructure, personal data, and business operations [2]. Attackers, trying to breach data in IoT environments, use advanced technology to take advantage of vulnerabilities in connected devices and networks. Attackers use highly developed malware and ransomware designed specifically for IoT devices. These harmful programs can get into IoT systems, encrypt data, and demand a ransom for decryption, leading to significant disruptions and financial consequences [3].

Using artificial intelligence (AI) can significantly improve the security of IoT systems, effectively preventing data theft, and protecting the integrity and confidentiality of sensitive information [4]. By learning the regular patterns of activity, machine learning-based IDS can uncover previously unnoticed threats and zero-day attacks by identifying anomalies in network traffic and user behavior, which might escape detection by rule-based systems [5]. In the context of intrusion detection, data can be very complex and unstructured, including network packets and log files. DL models show a remarkable ability to process such data, as they can capture intricate patterns and relationships effectively. This capability leads to improved accuracy in detecting sophisticated attacks [6, 7].

In general, IDS datasets consist of a collection of network traffic logs, system logs, security event logs, and other relevant data gathered from various network devices and systems. The large volume of these data presents challenges in

processing and analysis [8]. Various deep learning models have been applied in intrusion detection. Convolutional neural networks (CNNs) [9] can be used in intrusion detection to analyze network packet payloads or represent traffic data as images. They can identify patterns that signal attacks, making them effective in detecting intrusions within the network [10]. Recurrent neural networks (RNNs) have shown great promise in intrusion detection. Being good at processing sequential data, RNNs are well-suited for analyzing the time-series data frequently encountered in IoT networks [11]. Long–short-term memory (LSTM) networks are valuable in analyzing time-series data, such as network traffic or system logs, as they are good at capturing the temporal dependencies that exist within intrusion patterns [12]. Even though cutting-edge solutions do not align with the challenges posed by the rapidly increasing high-speed network traffic, to address these challenges in detecting intrusions we have designed an effective IDS involving recursive feature elimination and information gain (RFE-IG) and cascaded LSTM.

An IDS is a security solution crafted to oversee network traffic and monitor system activities, identifying any malicious activities or policy violations. Its primary role is to operate as a security shield, ensuring protection for computer systems and networks by preventing unauthorized access, misuse, and malicious activities. Managing data, detecting evolving cyber threats, and handling high-speed network traffic present notable challenges for IDS in IoT environments. The complexity and volume of data, alongside the emergence of sophisticated malware and the demands of rapidly increasing network activities, highlight critical areas for enhancing IDS methodologies and technologies to effectively safeguard against prevalent cyber threats. This article introduces a method for improved intrusion detection in network systems, utilizing a hybrid approach, RFE-IG, for effective data preprocessing and feature identification. Employing cascaded long–short-term memory (CLSTM) networks, which involve three LSTM layers, the proposed method not only detects but also accurately categorizes cyberattacks. Validated using NSL-KDD and UNSW-NB15 datasets, and compared with existing methods, the approach demonstrates both reliability and practicality in real-world scenarios, providing a sound and notably proficient strategy in intrusion detection.

The major contributions of the article are presented as follows:

(1) To handle huge volume of datasets with variety of attributes, a feature selection strategy involving RFE-IG is introduced to determine the most contributing features.

(2) To effectively identify the occurrence of intrusions, a novel Cascaded LSTM model is formulated stacking of three LSTM layers. The classifier is capable of detecting binary and multiclass attack categories from the reduced dataset.

(3) The performance evaluation of the proposed method is carried out with various existing methods and shows better intrusion detection capabilities for the given datasets.

The content of the article is structured as follows: The existing literatures are analyzed in Section 2. The methodology and the detailed working of proposed IDS are presented in Section 3. Section 4 details the working of IDS and performance evaluation with other methods. The last chapter describes the contribution of the article and the possible extension of it in future.

2. Related Work

Machine learning and deep learning algorithms have emerged as revolutionary technologies with diverse applications, presenting the opportunity to reshape industries, enhance decision-making processes, and tackle intricate challenges across multiple domains. This section deals with various models designed for IDS.

By utilizing feature selection techniques, IDS can identify the most relevant and informative features, effectively reducing the data's dimensionality. The features are optimized based on the correlation between the attributes and artificial neural networks is used to detect attacks [13]. The model produced an accuracy of 97.49% for NSLKDD dataset. Xboost method is used as classifier, and the structure of the Xboost is optimized using particle swarm optimization (PSO) [14]. The important features of KDDCUP'99 data are extracted using Binary Grey Wolf Optimizer (BGWO) and determine the occurrence of intrusion [15]. BGWO employs various number of wolves for feature reduction. An IDS is designed with Tabu Search for feature selection and RF for detection [16]. UNSWNB-15 dataset is used to validate and produced superior performance in terms of FPR and detection rate but suffers due to class imbalance problem. SA-ISSA method is employed to minimize the number of attributes and voting based on group of classifier involving LR, DT, KNN, SVM, and BiLSTM is used for detection [17]. The method achieved an accuracy of 96.4% for RPL-NIDDS17 dataset.

DL models have the capacity to grasp the regular behavior of a system or network and recognize deviations that signal potential intrusions or anomalies. A deep learning-based IDS involving LSTM, RNN, and GRU is used [18]. The model utilizes features decreased by Xboost method. The model produced an accuracy of 88.07% for UNSW-NB15 dataset. The model was not implemented to detect multiclass attack categories. A tree-based WFEU is used to select optimal features [19]. Further FDNN is used to determine attacks and reached accuracy above 99% for both binary and multiclass attack categories. An IDS model using double PSO for tuning parameters and selection of features is designed [20]. DNN, RNN, and DBN are used as classifier for the IDS. The model produced better FAR for NSL-KDD and CICIDS2017 datasets compared to other approaches. A hybrid method IGRF-RFE for choosing relevant features is performed [21]. The method detected the occurrence of attacks using MLP and showed an accuracy of 82.25% with 23 features for UNSW-NB15 dataset.

An OGBDT-based IDS model is designed with the composition of GAs and optimized GBTs. The optimization is performed with the support of enhanced African buffalo

Table 1: Review of existing literature.

Technique	Functionality	Pros	Cons
CNN	Automates feature extraction and can be adapted for classification	Pretrained CNN models save time and resources	Vulnerable to adversial attacks. CNNs can overfit the training data
RNN	Captures temporal dependencies in data and distinguish normal behavior from suspicious patterns	Adaptable to different types of network traffic patterns and diverse datasets	RNNs are prone to the vanishing gradient problem during back-propagation through time
GRU	GRUs utilize gating units to selectively manage and update information	Capable of understanding network activities by grasping long-term dependencies	GRUs are prone to overfitting while dealing with imbalanced datasets
Autoencoders	Autoencoders do not require labeled intrusion data for training	Well-suited for unsupervised learning, training autoencoders, especially deep ones, is complex	They do not perform as well in supervised learning tasks where labeled data are abundant
DBF	Use unsupervised learning to automatically learn hierarchical representations of data	Can adapt to evolving attack patterns, making them effective for detecting new attacks	Proper tuning of hyperparameters is essential. DBNs require large and diverse datasets
LSTM	Analyzes sequential network data to detect patterns, anomalies, and identify cyber threats effectively	Captures long-term dependencies in sequential data to understand network activities' context effectively	LSTM is vulnerable to adversial attacks. Response time is high for large-scale networks

optimizations [22]. A hybrid IDS involving LSTM and GRU is formulated with features chosen based on correlation among attributes and validated using CICIDS 2017 dataset and showed good results for binary classification and lacked in performance for multiclass classification [23]. In order to check for intrusion in IOT environment where the necessary features of the input dataset are extracted using MBGO. Further attention-based LSTM checks for the possibility of attacks, and the parameters are effectively determined by AO scheme [24]. The method showed reduced false rate for NSLKDD dataset. A hybrid IDS is designed with modified GTO–BSO for retrieving essential features. The performance of the method is improved using BSA algorithm [25]. The method was compared with multiple approaches against various dataset.

By iteratively exploring diverse feature subsets and evaluating their performance, wrapper methods ascertain the most informative combination of features [26]. An IDS is designed with dual CNN, the former to select the attributes and the later for classification [27]. The FPR of this method is 1.9% for BoT IoT 2020 dataset. The model was not validated for multiclass attack detection. An IDS is designed involving DNN-based model [28]. The PCA method reduced the input size and further optimized using GWO. The detection of attack in reduced dataset is carried out using DNN. Multiple classifiers including RF, MLP, and CNN models are incorporated to design detection of intrusions [29]. CNN model has the highest accuracy of above 90% with 10 epochs with training time less than a minute. The model was designed to detect only DOS attacks. A hybrid IDS is created involving ELSTM and RNN approaches [30]. The IDS processes the data reduced using LPPSO method. A combination of IG and PCA is applied to reduce the dataset and a combination of IBK, SVM, and MLP is formulated to classify the attacks based on the aggregation of the classifiers [31]. Stacked deep-learning models have shown improved performance [32]. Continued research and development in intrusion detection are vital to navigate the constantly evolving cyber threat landscape. Both organizations and individuals need to take active cybersecurity steps, including regular software updates, enforcing robust security protocols, and staying current with threats and defense methods. As new attack and intrusion methods emerge, presenting challenges to existing models, the creation of new models helps security researchers effectively address these changing threats. A table summarizing the functionality of various techniques from the literature is presented in Table 1.

Ensuring the safety of IoT is critical due to its widespread use and the sensitive data it manages. While various algorithms have been employed to enhance IDS, handling large datasets, and accurately identifying cyber threats in a timely manner remains a challenge. RFE systematically explores diverse feature combinations, conducting an exhaustive search across the feature space. By evaluating subsets of features and considering intricate feature interactions, RFE enables a comprehensive dataset analysis. Notably, RFE adeptly manages multicollinearity, effectively addressing high correlations between features. This capability ensures a robust and accurate selection of relevant features suitable for IDS. Our proposed approach utilizes LSTM networks, specifically CLSTM method. Cascaded LSTMs excel at capturing prolonged sequences of events, making them ideal for intrusion detection. With 60% of features chosen from the input dataset using RFE-IG improves the performance of IDS and eliminates overfitting. Thus, CLSTM helps in detecting attacks that develop gradually, enabling the system to identify various types of new attacks.

3. Materials and Methods

In IOT, diverse forms of attacks can profoundly affect both individual devices and the broader interconnected network. IOT network is vulnerable to variety attacks like Denial of Service, Distributed Denial of Service, botnets, ransomware,

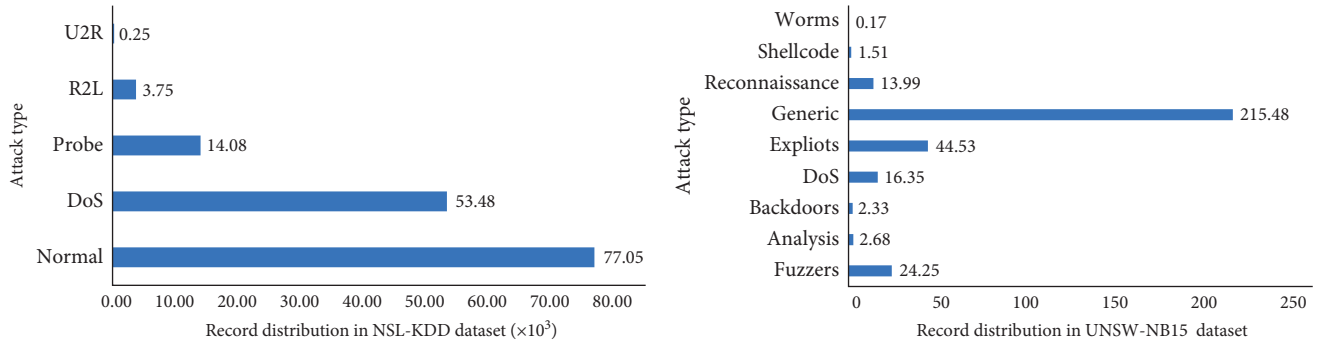


Figure 1: Distribution of records: (a) NSL-KDD and (b) UNSW-NB15 dataset.

zero-day attacks Man-in-the-Middle attack. Security breaches through various attacks can result in compromised data integrity, unauthorized access, service disruptions, privacy violations, financial losses, device damage, and even potential physical harm, underscoring the essential requirement for strong security protocols in IoT systems.

In conducting this study, we utilized a robust computational setup comprising an Intel Core i7-9700K CPU with 32 GB DDR4 RAM and a 1TB SSD, running on Ubuntu 20.04 LTS. The feature selection and cascaded LSTM model development were implemented using Python 3.8, leveraging libraries such as Scikit-learn for RFE-IG and TensorFlow for modeling. This setup ensured efficient handling of the NSL-KDD and UNSW-NB15 datasets, facilitating high-accuracy binary classification results.

3.1. Dataset Details. The NSL-KDD dataset has been altered from the original KDD Cup 1999 dataset to offer a more realistic depiction of contemporary network traffic. The dataset is widely accepted in the research community as a standardized benchmark for evaluating the performance of intrusion detection and network security algorithms [33]. The dataset encompasses a variety of network activities, including normal traffic and diverse attack types like denial of service (DoS), probe, remote to local (R2L), and user to root (U2R) attacks. This diversity ensures its portrayal of real-world network scenarios. Each network connection instance in the NSL-KDD dataset is described by 41 features that represent various characteristics of network traffic. These features serve as inputs to intrusion detection and network security algorithms.

The UNSW-NB15 dataset, provided by the University of New South Wales (UNSW) in Australia, is a benchmark dataset specifically utilized by researchers for IDS and other network security algorithms. The dataset contains genuine network traffic data, offering a pertinent and precise depiction of the current cyber threat landscape. The UNSW-NB15 dataset encompasses nine distinct attack categories providing a broad spectrum of cyber threats. Each network connection instance in the dataset is described by 47 features. Features such as duration, protocol_type, and service from the NSL-KDD dataset, along with srcip, dstip, and state from the UNSW-NB15 dataset, are emphasized for their critical roles in identifying network threats. This analysis supports the strategy of leveraging these datasets to develop robust IDS, thereby enhancing the capability to effectively detect and mitigate cyber threats in IoT networks. The distribution among the categories of attack is presented in Figure 1.

3.2. Proposed Workflow. The proposed IDS scheme takes the NSL-KDD and UNSW-NB15 data records as the input. The first stage is preprocessing of input data. The categorical information is transferred into numeric information using Label Encoder. Max–min Normalization is employed to scale the features of the input dataset. Further the input data are divided into training and testing data. The overview of the proposed model is depicted in Figure 2. RFE-IG-based feature selection is performed to determine the necessary features and to avoid overfitting. Further cascaded LSTM model is trained using training data. The performance of the model is validated using the test data.

3.3. RFE-IG for Feature Selection. RFE stands as a valuable tool in machine learning, sought after for its ability to bolster model performance and improve understandability by singling out the most essential features. In a stepwise manner, RFE prunes away the least pertinent features from the dataset until either a predefined feature count is attained or the model's performance reaches an optimal state. This streamlining process not only helps prevent overfitting but also enhances model interpretability, enabling a clearer grasp of the underlying data patterns and driving more insightful analyses [34]. Through the elimination of less informative features, RFE enables the IDS to concentrate on the most pertinent aspects of the data. Consequently, the IDS becomes more proficient in detecting novel intrusion patterns, enhancing its ability to generalize to new and unseen data [35].

RFE works through a step-by-step process of removing the least important features and retraining the model. By adopting this systematic strategy, RFE ensures that the most relevant features are preserved, leading to improved model performance using random forest. The iterative elimination and retraining process continues until either the desired number of features is achieved or the model achieves a satisfactory level of performance.

Random forest begins by dividing the original dataset into several subsets using a method called bootstrapped

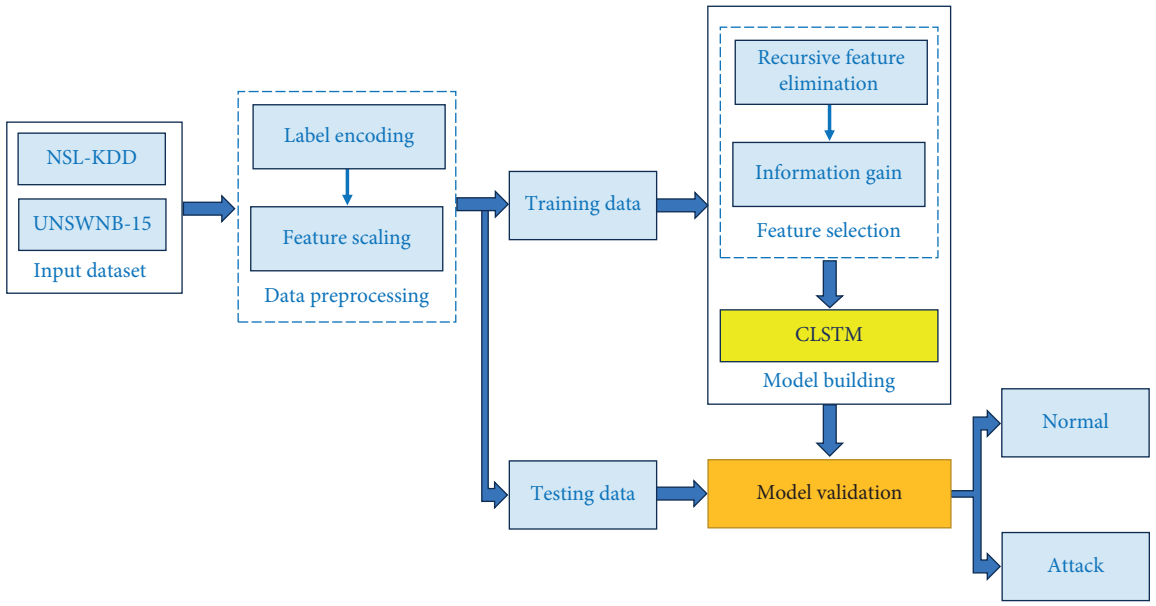


Figure 2: Overview of the proposed IDS.

sampling. In this process, data points are randomly selected with replacement to form each subset. These subsets serve as the training data for individual decision trees. Every tree is constructed by choosing the optimal feature from a randomly selected subset of features at each node. At every node in the tree, a random subset of k features is selected from the n features in the dataset. The importance of feature fi is computed as follows:

$$\mathrm{IS}(\mathrm{fi}) = \sum_{t=1}^{T} \frac{\text{Impurity decrease}_t(\mathrm{fi})}{T}, \tag{1}$$

where fi denotes the ith feature, number of trees in RF is T, and the impurity caused by feature fi is denoted as impurity decrease (fi).

The feature selection happens in two stages. Initial level of features is selected by RFE algorithm, and final level of features is selected by using IG algorithm. The algorithm explaining the stage wise feature selection process is explained in Algorithm 1.

IG aids in the identification of features that offer the greatest insight into the class labels, rendering them strong contenders for dividing the dataset. Features demonstrating greater IG are prioritized because they result in more substantial reductions in entropy, ultimately contributing to the creation of more effective models for classification purposes. IG measures how effectively a specific feature, when employed to divide the dataset, decreases its entropy. The entropy is defined using Equation (2):

$$\mathrm{Entropy}(F) = -\sum \mathrm{fi} \times \log_2 p(\mathrm{fi}), \tag{2}$$

where p(fi) is the probability of occurrence of fi.

A higher IG indicates that the feature holds greater value in classifying the data. IG is computed using Equation (3):

$$\mathrm{IG}(\mathrm{Fi}) = \mathrm{Entropy}(F) - \sum v \in \mathrm{values}(F) \left(\frac{|F'|}{|F|}\right) \times \mathrm{entropy}(F'), \tag{3}$$

where values (F) are the possible values of the feature F and F' being the subset of F.

The proposed scheme utilizes IG to determine the features having higher correlation for the features selected using RFE. This further eliminates the features having least IG score. The selected feature set is further utilized by cascaded LSTM model to determine the occurrence of attack in the network.

3.4. Cascaded LSTM Classifier. The proposed IDS model employs the LSTM model to effectively identify intrusions. The features of the input dataset, reduced using the RF-RFE-IG method, are processed by the LSTM to detect the occurrence of attacks. The proficiency of LSTMs in preserving and adjusting information across lengthy sequences gives them an exceptional ability to recognize patterns. A cascaded LSTM model is a neural network design that entails the layering of multiple LSTM components, one atop the other. The proposed model uses cascaded LSTM comprising of three LSTM layers. The layer stack arrangement of CLSTM is presented in Figure 3.

This makes them suitable for a range of applications, including IDS. An overview of the LSTM network is depicted in Figure 4. The functioning of the LSTM involves input, output, and forget gates. This section might be divided into subheadings. It should provide a concise and precise description

Feature selection Stage 1: RFE Algorithm

1. **Initialization**:

I. **Feature set**: Let F denotes the features where $F = \{f1, f2, \ldots fn\}$, n is the total no of features.

II. **Initialize**: The selected the features F' with all the features of F.

III. **Specify**: Let k be the number of features to be selected.

IV. **Elimination**: Let D represents the list of eliminated features.

2. **Feature Selection:**

I. **Perform**: Until the features in F' is greater than k perform: 1–4

1. **Train** the RF model with the features of F'.
2. **Compute** the feature importance score of the features in F' as IS(f).
3. **Rank** the features of F' Rank(fi) based on the importance score IS(f).
4. **Remove** the least important n–k features from F'. Update the eliminated features in D.

3. **RFE Selected Features:**

I. **Initial Elimination**: The features in F' denote the selected features and D provides the eliminated features.

Feature selection Stage 2: IG Algorithm

4. **Initialization**:

I. **Feature set**: Let F' denotes the input dataset with $F' = \{f1, f2, \ldots fn–k\}$.

II. **Initialize**: The selected features F'' with all the features of F'.

III. **Specify:** Let k' be the number of features to be selected.

IV. **Elimination**: Let D' represents the features eliminated using IG.

5. **Feature Selection:**

I. **Compute** the entropy of features in F''.

II. **Compute** the information gain IG of each feature in F''.

III. **Rank** the features of F'' using the IG score.

IV. **Remove** the least important n–k–k' features from F''. Update the eliminated features in D'.

6. **RFE-IG Selected Features:**

I. **Final Elimination**: The features in F'' denotes the selected features and D' provides the eliminated features.

Algorithm 1: Stage wise feature selection.

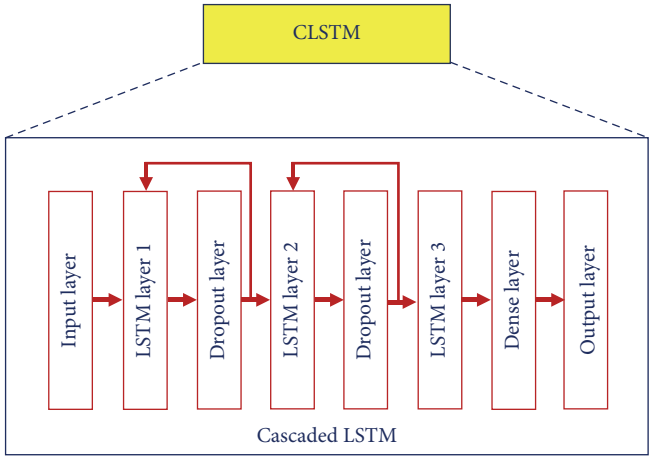


Figure 3: Layer stack arrangement of cascaded LSTM.

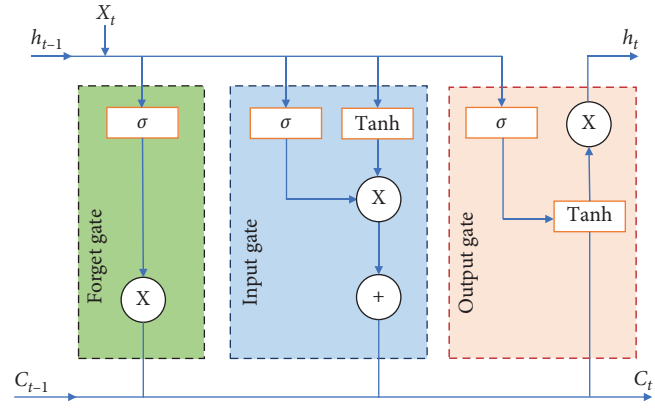


Figure 4: Overview of LSTM network.

of the experimental results, their interpretation, and the conclusions that can be drawn from the experiments.

Central to the mechanism of the LSTM is the input gate. This gate determines the amount of new data incorporated into the memory cell at each time step. By evaluating the importance of the current input data, the input gate enables the LSTM to strengthen its memory selectively while retaining essential information. The input gate function I_t is calculated using the current state X_t and the previous hidden state h_{t-1} at every time step t and represented using Equation (4):

$$I_t = \mathrm{Sig}(W_i[h_{t-1} \otimes X_t] + b_i). \quad (4)$$

The candidate value in input gate is computed using the following equation:

$$\check{C}_t = \tan(W_c[h_{t-1} \otimes X_t] + b_c), \quad (5)$$

where the weight factors are denoted using W_i and W_c, and b_i and b_c are the bias of the input cell.

After combining the weighted inputs and bias, they undergo a sigmoid activation function, compressing the values to fall within the range of 0–1. As a result of employing tanh function, the newly introduced information will exhibit values within the range of −1 to 1. The value is added to cell while it is positive and ignored if it is negative.

The forget gate holds significant importance within a LSTM network, as it dictates the degree to which previously stored data are either maintained or excluded from the memory cell. Its crucial function empowers LSTMs to acquire and apprehend patterns within data across extensive time intervals. At each time step, the LSTM utilizes the current input data x_t and the previous hidden state h_{t-1} and forget gate is computed using the following equation:

$$F_t = \mathrm{Sig}\big(W_f[h_{t-1} \otimes X_t] + b_f\big), \quad (6)$$

where b_f and W_f represent the bias value and weight factors of forget gate, respectively. The forget gate activation operates on each element of the preceding memory cell state C_{t-1} independently via element-wise multiplication. This procedure dictates which segments of the memory cell state to be maintained and which should be disregarded. The final configuration of the updated memory cell state C_t is molded by the dynamic interplay among the memory cell update, the candidate cell state $\check{C}_t$ and the input gate I_t.

The output gate O_t regulates the transfer of information from the memory cell to either the output or the subsequent hidden state. This gate plays a crucial role in determining the data that should be unveiled as the final LSTM output in each step and is determined using the following equation:

$$O_t = \mathrm{Sig}(W_o[h_{t-1} \otimes X_t] + b_o). \quad (7)$$

The weight parameter is W_o and the bias vector is b_o. The modified hidden state h_t can serve as the point of origin for the LSTM output in the current time step t, or it can alternatively be passed on to the subsequent network layer for additional enhancement and is denoted using the following equation

$$h_t = O_t \otimes \tanh(C_t). \quad (8)$$

Through dynamic modulation of the input gate activation, the LSTM becomes adept at capturing significant patterns and interconnections within the data. In the cascaded LSTM architecture presented, a strategic dropout layer is introduced between LSTM layers to prevent overfitting by randomly omitting subsets of features during training. This technique, combined with feedback recycling to the LSTM layer, fosters robust regularization and model generalization. Hyperparameters, including a 0.5 dropout rate and early stopping, were meticulously optimized to enhance IDS performance, achieving significant accuracies on NSL-KDD and UNSW-NB15 datasets.

Throughout the forward pass, the input data are subjected to processing within the LSTM layers, resulting in the formation of predictions. Each LSTM unit within the network maintains its inherent state, facilitating the ability to comprehend and retain meaningful patterns within sequential data. The effectiveness of the model's prediction is estimated using mean square error (MSE) which is given by the following equation:

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(x_i - \check{x})^2, \quad (9)$$

where $\check{x}$ is the prediction of the LSTM model and x is the actual value in the dataset. By squaring the values during the RMSE calculation, larger errors receive more emphasis than smaller errors. RMSE is determined using the following equation:

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \check{x})^2}. \quad (10)$$

After calculating the loss, LSTM initiates backpropagation to calculate gradients for the loss in relation to the weights and biases at each discrete time step. Through the process of backpropagation, the network gains the ability to learn from errors and progressively enhance its predictive capabilities over a period of time. The parameters are tuned to reduce the loss of the model.

Utilizing cascaded LSTM for intrusion detection with the UNSW-NB15 and NSL-KDD datasets has the potential to enhance accuracy and resilience in recognizing network intrusions and anomalies, consequently bolstering the comprehensive security of network systems.

4. Results and Discussion

4.1. Feature Selection Using RFE-IG Method. The proposed method utilizes RFE-IG method to select the most important features of the input date for further processing. The cascaded LSTM model has shown better performance with reduced features in detecting attacks. The feature selection scheme selects 30 features among the 41 features of NSL-KDD dataset. The reduced dataset is further processed and the 25 features out of it are found to be the most contributing features. The list of features determined using RFE-IG for NSLKDD dataset is presented in Figure 5.

The UNSW-NB15 dataset consists of 47 features. On processing the dataset with RFE scheme, the method identifies 30 features from the dataset based on feature importance score. In every iteration RFE eliminates the least important

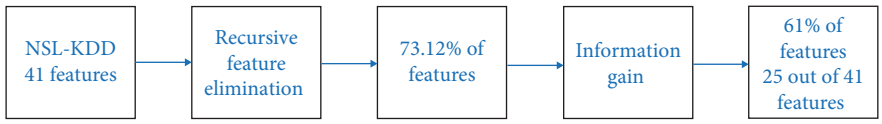


Figure 5: Details of features selected from NSL-KDD dataset.

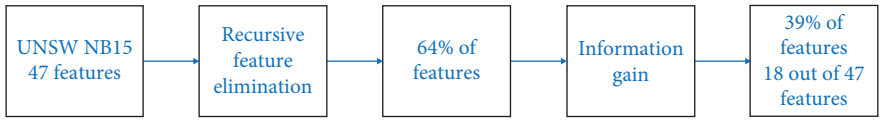


Figure 6: Details of features selected from UNSW-NB15 dataset.

Table 2: Performance metrics.

Metrics	Formula
Accuracy: Quantifies the fraction of accurately categorized instances among the entire set	$\text{Accuracy (A)} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$
Precision: Determines the fraction of accurate positive forecasts in relation to the total positive forecasts	$\text{Precision (P)} = \text{TP}/(\text{TP} + \text{FP})$
Recall: Quantifies the relationship between accurate positive predictions and the overall number of actual positive instances	$\text{Recall (R)} = \text{TP}/(\text{TP} + \text{FN})$
F1-score: Strikes a balance between precision and recall by taking their harmonic mean	$\text{F1} - \text{score} = 2 \times (\text{P} \times \text{R})/(\text{P} + \text{R})$

features. The features primarily selected by RFE are processed using IG to further identify the contributing features of the input dataset. The method reduced the number of features to 18 and details are presented in Figure 6. The reduced features are processed further to train the cascaded LSTM model to detect the occurrence of attack.

RFE is a methodical procedure for feature selection that progressively trims less significant features from a dataset, leading to a more compact and informative feature subset suitable for training machine learning models. Combining IG with RFE ensures that the feature selection process is guided by the importance of each feature with respect to the target variable while also considering its impact on the model's predictive performance. This approach helps identify a subset of features that not only contain valuable information but also improve the detection rate of IDS.

4.2. Performance Metrics. Evaluating the effectiveness of IDS is pivotal for accurate identification and classification of security threats. This evaluation involves employing binary classification, discerning normal from malicious activities, as well as multiclass classification, categorizing diverse attack types. Binary classification is instrumental in discerning between typical network behavior and potential intrusions or attacks. This approach offers a definitive assessment, indicating whether a specific activity is malicious or benign with precision. Multiclass classification empowers the IDS to accurately categorize diverse attack types such as DoS, probing, and malware. This precise categorization is invaluable, enabling targeted responses and facilitating focused security enhancements tailored to specific attack patterns. Table 2 presents the performance metrics that are used to evaluate the proposed method.

4.3. Binary Classification. The reduced features chosen using RFE-IF are fed to cascaded LSTM to detect for occurrence attacks. Initially binary classification is carried out to detect normal and attack classes. The confusion matrix is utilized to determine the performance metrics of the machine learning model. The confusion matrix for binary classification against NSL-KDD and UNSW-NB15 datasets is presented in Figure 7. From the confusion matrix, it is clearly observed that the proposed scheme has the ability to rightly identify the attack and normal classes.

The performance of the proposed method is evaluated using the components of confusion matrix. The performance of proposed approach with reduced features is presented in Figure 8. The accuracy of performing binary classification is 98.96% and 99.3% for NSL KDD and UNSW-NB15 datasets. The ability of proposed method in detecting attack and normal class is 99.04% and 99.45%. The method records minimal FPR of 1.13 and 1.1% for NSL-KDD and UNSW-NB15 datasets, respectively.

The loss and accuracy of proposed method for training and testing data are presented in Figure 9. The ROC curve depicts how well a classification model performs at different discrimination thresholds, showing the balance between true positive rate and false positive rate across a range of threshold values. The ROC curve of the proposed scheme for performing binary classification using NSL-KDD dataset is presented in Figure 10.

4.4. Multiclass Classification. The NSL-KDD dataset is composed of multiple categories of attacks. All these attacks are grouped under four categories namely DoS, probe, R2L, and U2R. The performance of proposed approach for NSL-KDD dataset in performing multiclass classification is presented in

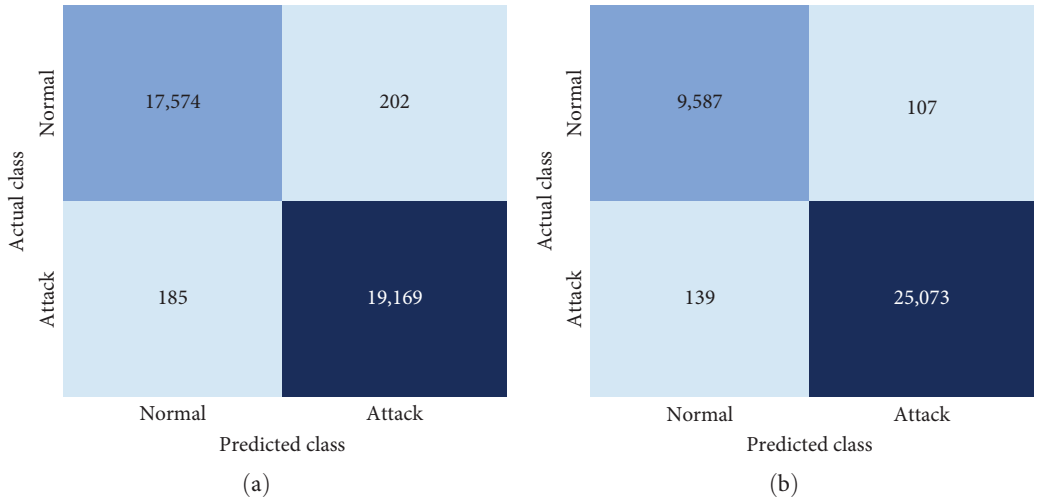


Figure 7: Confusion matrix of binary classification: (a) NS-KDD dataset and (b) UNSW-NB15 dataset.

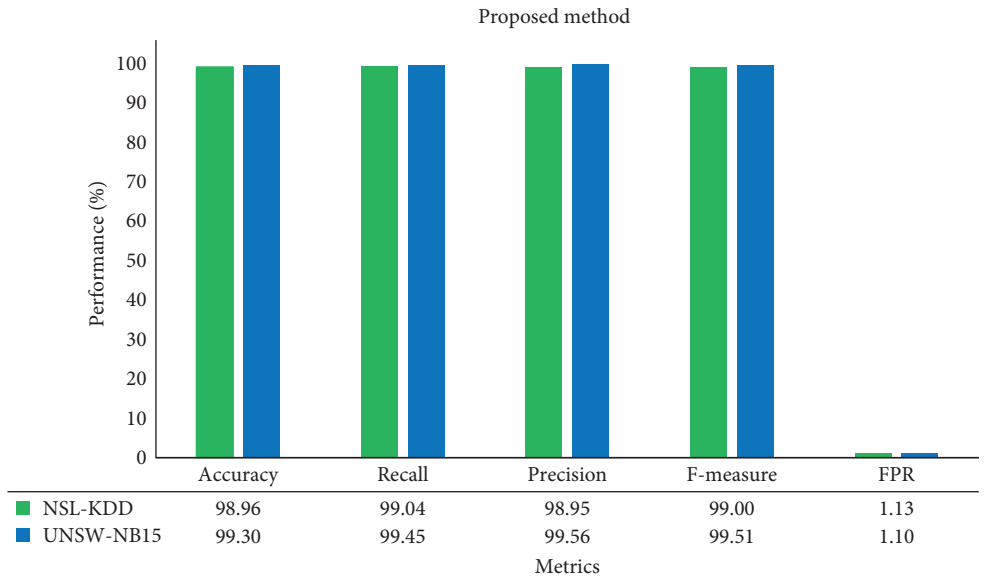


Figure 8: Binary classification performance of proposed method.

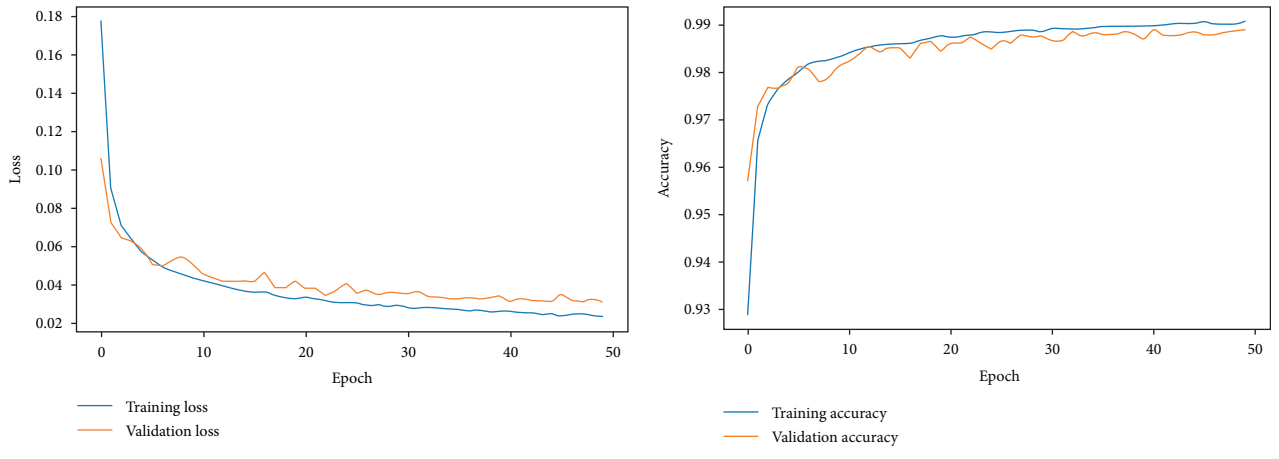


Figure 9: Training vs. validation performance: (a) loss and (b) accuracy.

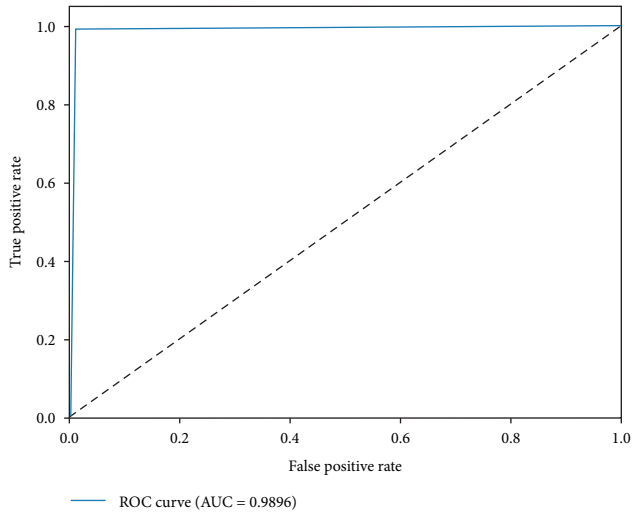


Figure 10: ROC curve for NSL-KDD dataset.

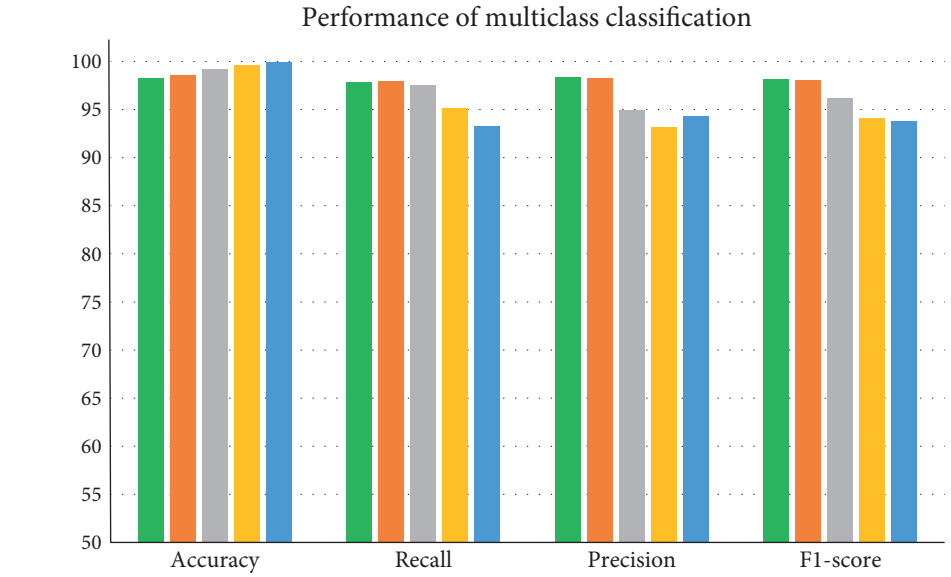
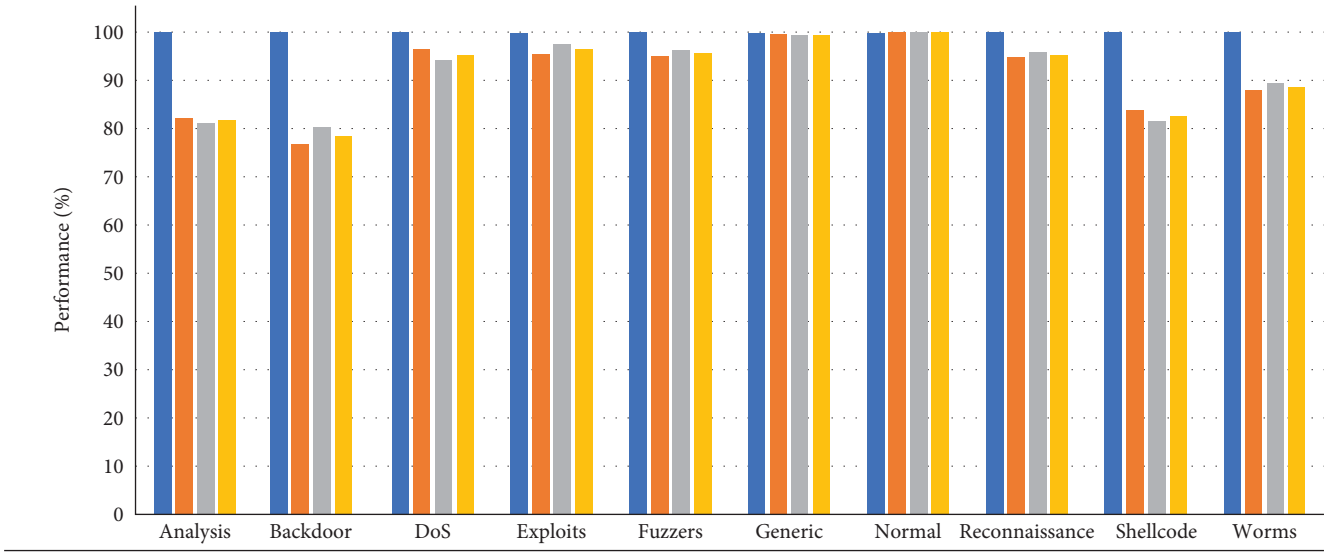


Figure 11: Performance of multiclass classification for NSL-KDD dataset.

Figure 11. The accuracy is 98.23% and 98.57% for detecting normal and DoS classes, respectively. The accuracy is 99.17% for probe category, whereas the accuracy is 99.59% for R2L type of attack class.

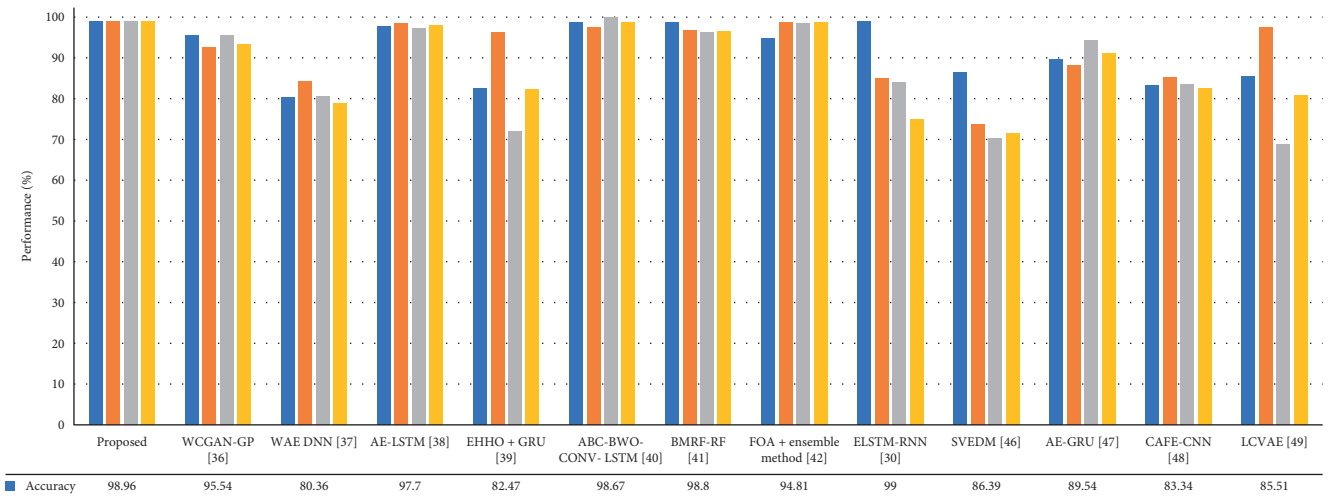
The UNSW-NB15 dataset consists of various category of attacks which are majorly grouped into 10 categories. The effectiveness of the proposed approach has been verified in identifying various multiclass attack types, and the results are presented in Figure 12. The proposed method produced an accuracy close to 1 in detecting all types of attacks. Similarly the recall value is 96.38%, 99.53%, and 99.96% for DoS, generic, and normal attack types, respectively. The method produced precision value of 94.11% for DoS and 99.41% for generic class, respectively.

4.5. Performance Comparison. To the evaluate the performance, the proposed method is compared with various existing methods. The performance comparison for binary classification of NSL-KDD dataset is presented in Figure 13. Among the compared methods, the performance of BMRF-RF and ABC-BWO-CONV-LSTM methods produced accuracy closer to the proposed approach. The proposed method



	Analysis	Backdoor	DoS	Exploits	Fuzzers	Generic	Normal	Reconnaissance	Shellcode	Worms
Accuracy	99.96	99.97	99.94	99.88	99.92	99.91	99.90	99.95	99.99	99.99
Recall	82.14	76.81	96.38	95.53	95.04	99.53	99.96	94.74	83.78	87.93
Precision	81.18	80.30	94.11	97.45	96.32	99.41	99.93	95.90	81.58	89.47
F1-score	81.66	78.52	95.23	96.48	95.67	99.47	99.94	95.32	82.67	88.70

Figure 12: Performance of multiclass classification for UNSW-NB15 dataset.



	Proposed	WCGAN-GP [36]	WAE DNN [37]	AE-LSTM [38]	EHHO + GRU [39]	ABC-BWO-CONV- LSTM [40]	BMRF-RF [41]	FOA + ensemble method [42]	ELSTM-RNN [30]	SVEDM [46]	AE-GRU [47]	CAFE-CNN [48]	LCVAE [49]
Accuracy	98.96	95.54	80.36	97.7	82.47	98.67	98.8	94.81	99	86.39	89.54	83.34	85.51
Precision	99.04	92.61	84.17	98.6	96.23	97.48	96.8	98.68	85	73.62	88.13	85.35	97.61
Recall	98.95	95.54	80.61	97.2	72.02	100	96.2	98.46	84	70.22	94.34	83.44	68.9
F1-score	99	93.41	78.8	97.9	82.38	98.73	96.5	98.68	75	71.49	91.13	82.6	80.78

Figure 13: Binary classification performance comparison for NSL-KDD dataset.

is superior in performance than all other approaches. Similarly, the recall value of ABC-BWO-CONV-LSTM approach is superior than the proposed approach but still the proposed approach is better with the values precision and F-score. The accuracy of ELSTM-RNN method is slightly superior than the proposed approach, but lacks in terms of precision and recall and F1-score with a difference of 14%, 14.95%, and 24%, respectively.

The performance of proposed method for UNSW-NB15 dataset is evaluated against various existing methods and their performance measures are presented in Figure 14. It is clearly evident that the proposed method outperforms the existing approaches. Among the compared methods, the ABC-BWO-CONV-LSTM method showed performance closer to the proposed approach. The method showed significant improvement than other approaches. The FOA + ensemble method produced precision value of 0.23% better than proposed approach, but the proposed method produced improvement of 0.41%, 0.24%, and 0.6% in terms of accuracy, recall, and F1-score, respectively, for UNSW-NB15 dataset.

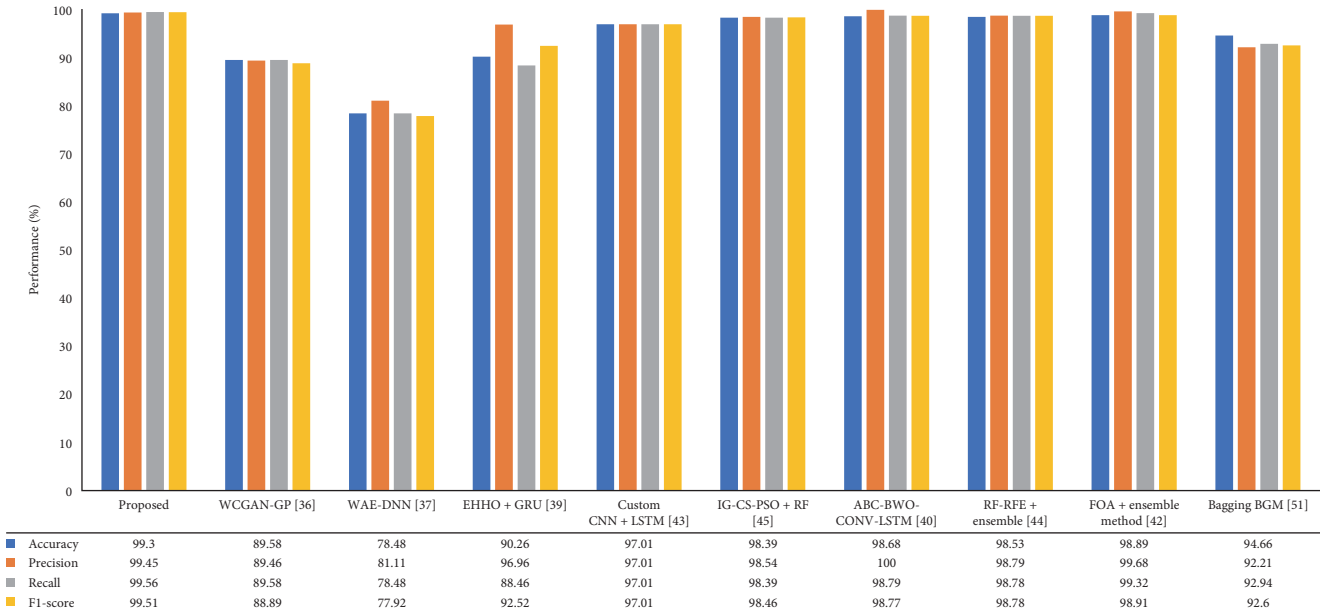


Figure 14: Binary classification performance comparison for UNSW-NB15 dataset.

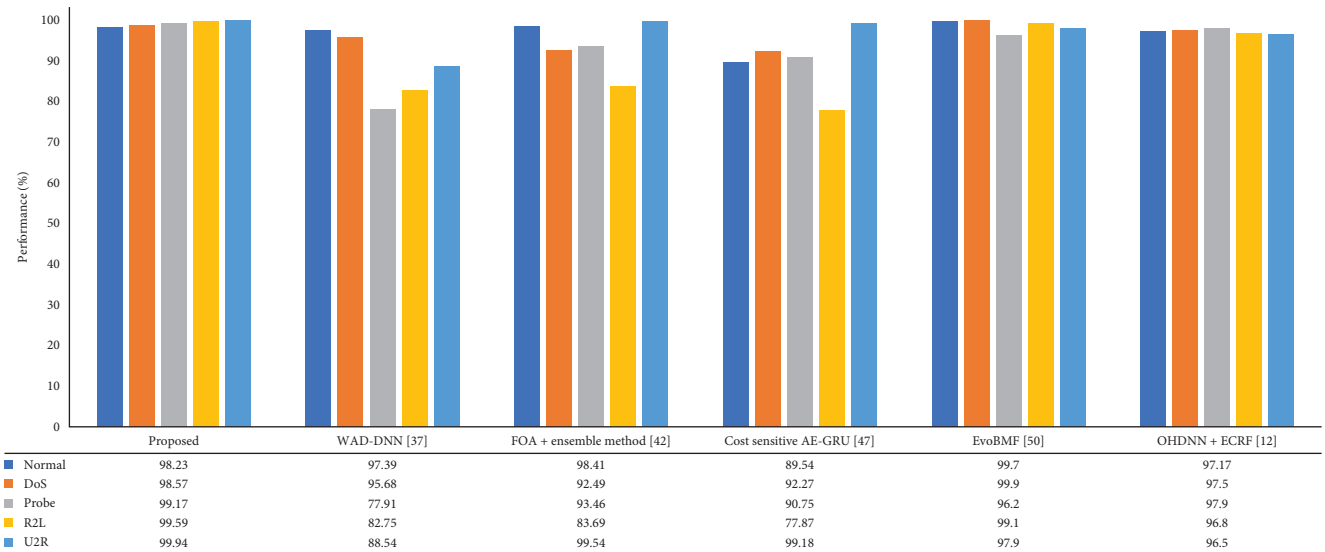


Figure 15: Multiclass classification accuracy comparison for NSL-KDD dataset.

The performance of proposed approach in detecting multiclass attack categories of NSL-KDD dataset is evaluated comparing with existing approaches. The performance comparison is presented in Figure 15. The accuracy of proposed method is above 99% of all categories of attacks. Among the compared methods FOA + Ensemble method and cost effective AE-GRU method had produced accuracy close to proposed method in determining U2R attacks. However, these methods lacked in determining the other categories of attacks.

On evaluating the results with the existing approaches, it is observed that the proposed method is producing superior results for binary and multiclass classification among the two standard datasets. Overall the proposed method is well suited in determining all sorts of attacks.

5. Conclusion

This study introduces a novel IDS model that utilizes a hybrid feature selection method combining RFE and IG techniques. The strength of this approach is evident in its ability to both enhance intrusion detection accuracy and simplify dataset features effectively. When evaluated using well-known benchmarks such as the NSL-KDD and UNSW-NB15 datasets, the proposed model achieved impressive accuracy rates of 98.96% and 99.3%, respectively. Importantly, these results were realized with a considerable reduction in input data, using only 69% of features for the NSL-KDD dataset and 39% for the UNSW-NB15. In addition to binary classification, the model effectively identified specific attack categories within these datasets.

As the reach of IoT networks grows, the need for efficient IDS like the one presented in this study becomes increasingly critical. Future research efforts will focus on balancing attack category distributions in datasets. This refinement is expected to enhance the model's performance, strengthening its relevance in real-world network security scenarios, particularly in the expanding domain of IoT.

Abbreviations

IDS: Intrusion detection system
RFE: Recursive feature elimination
IG: Information gain
LSTM: Long–short-term memory
CLSTM: Cascaded long–short-term memory
AI: Artificial intelligence
ML: Machine learning
DL: Deep learning
DNN: Deep neural networks
CNN: Convolutional neural networks
RNN: Recurrent neural networks
U2R: User to root
R2L: Remote to local
DoS: Denial of service
MSE: Mean square error
RMSE: Root mean square error
F': Subset of feature set S
X_t: Current state of LSTM
I_t: Input gate function
W_i: Weight factor
bi: Bias of input cell
TP: True positive
FP: False positive
TN: True negative
FN: False negative.

Data Availability

The NSL-KDD dataset is available at https://www.unb.ca/cic/datasets/nsl.html. The UNSW-NB15 dataset is available at https://research.unsw.edu.au/projects/unsw-nb15-dataset.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] M. Ali, M.-U. Haque, M. H. Durad et al., "Effective network intrusion detection using stacking-based ensemble approach," *International Journal of Information Security*, vol. 22, pp. 1781–1798, 2023.

[2] C. Zhang, Z. Lian, H. Huang, and C. Su, "PCIDS: permission and credibility-based intrusion detection system in IoT gateways," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 904–913, 2024.

[3] N. Elmrabit, F. Zhou, F. Li, and H. Zhou, "Evaluation of machine learning algorithms for anomaly detection," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–8, IEEE, Dublin, Ireland, June 2020.

[4] G. De Carvalho Bertoli, L. A. Pereira Junior, O. Saotome et al., "An end-to-end framework for machine learning-based network intrusion detection system," *IEEE Access*, vol. 9, pp. 106790–106805, 2021.

[5] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, Article ID e4150, 2021.

[6] M. Al Lail, A. Garcia, and S. Olivo, "Machine learning for network intrusion detection—a comparative study," *Future Internet*, vol. 15, no. 7, Article ID 243, 2023.

[7] A. A. Hagar and B. W. Gawali, "Apache spark and deep learning models for high-performance network intrusion detection using CSE-CIC-IDS2018," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 3131153, 11 pages, 2022.

[8] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, "Intelligent intrusion detection system for VANET using machine learning and deep learning approaches," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5069104, 13 pages, 2022.

[9] B. Kim, K. R. S. Preethaa, Z. Chen, Y. Natarajan, G. Wadhwa, and H. M. Lee, "Predicting the lateral displacement of tall buildings using an LSTM-based deep learning approach," *Wind and Structures*, vol. 36, no. 6, pp. 379–392, 2023.

[10] F. Zhai, T. Yang, H. Chen, B. He, and S. Li, "Intrusion detection method based on CNN–GRU–FL in a smart grid environment," *Electronics*, vol. 12, no. 5, Article ID 1164, 2023.

[11] S. H. Park, H. J. Park, and Y.-J. Choi, "RNN-based prediction for network intrusion detection," in *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pp. 572–574, IEEE, Fukuoka, Japan, February 2020.

[12] S. Karthic and S. M. Kumar, "Hybrid optimized deep neural network with enhanced conditional random field based intrusion detection on wireless sensor network," *Neural Processing Letters*, vol. 55, pp. 459–479, 2023.

[13] I. S. Thaseen, J. S. Banu, K. Lavanya, M. R. Ghalib, and K. Abhishek, "An integrated intrusion detection system using correlation-based feature selection and artificial neural network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Article ID e4014, 2021.

[14] H. Jiang, Z. He, G. Ye, and H. Zhang, "Network intrusion detection based on PSO-Xgboost model," *IEEE Access*, vol. 8, pp. 58392–58401, 2020.

[15] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1559–1576, 2021.

[16] A. Nazir and R. A. Khan, "A novel combinatorial optimization based feature selection method for network intrusion detection," *Computers & Security*, vol. 102, Article ID 102164, 2021.

[17] P. J. Prakash and B. Lalitha, "Optimized ensemble classifier based network intrusion detection system for RPL based internet of things," *Wireless Personal Communications*, vol. 125, pp. 3603–3626, 2022.

[18] S. M. Kasongo, "A deep learning technique for intrusion detection system using a recurrent neural networks based framework," *Computer Communications*, vol. 199, pp. 113–125, 2023.

[19] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion

detection system," *Computers & Security*, vol. 92, Article ID 101752, 2020.

[20] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," *Computer Networks*, vol. 168, Article ID 107042, 2020.

[21] Y. Yin, J. Jang-Jaccard, W. Xu et al., "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *Journal of Big Data*, vol. 10, Article ID 15, 2023.

[22] S. Mishra, "An optimized gradient boost decision tree using enhanced african buffalo optimization method for cyber security intrusion detection," *Applied Sciences*, vol. 12, no. 24, Article ID 12591, 2022.

[23] S. K. Gautam, A. Henry, M. Zuhair, M. Rashid, A. R. Javed, and P. K. R. Maddikunta, "A composite approach of intrusion detection systems: hybrid RNN and correlation-based feature optimization," *Electronics*, vol. 11, no. 21, Article ID 3529, 2022.

[24] M. A. Duhayyim, J. S. Alzahrani, H. A. Mengash et al., "Modified garden balsan optimization based machine learning for intrusion detection," *Computer Systems Science and Engineering*, vol. 46, no. 2, pp. 1471–1485, 2023.

[25] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry, "An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection," *Sensors*, vol. 22, no. 4, Article ID 1396, 2022.

[26] J. Maldonado, M. C. Riff, and B. Neveu, "A review of recent approaches on wrapper feature selection for intrusion detection," *Expert Systems with Applications*, vol. 198, Article ID 116822, 2022.

[27] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: dual convolutional neural network approach for feature selection and attack detection on internet of things networks," *Sensors*, vol. 23, no. 14, Article ID 6507, 2023.

[28] S. P. R. M., P. K. R. Maddikunta, P. M. et al., "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139–149, 2020.

[29] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," *Information*, vol. 11, no. 5, Article ID 279, 2020.

[30] A. A. E.-B. Donkol, A. G. Hafez, A. I. Hussein, and M. M. Mabrook, "Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks," *IEEE Access*, vol. 11, pp. 9469–9482, 2023.

[31] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," *Computer Networks*, vol. 148, pp. 164–175, 2019.

[32] S. Preethaa, Y. Natarajan, A. P. Rathinakumar et al., "A stacked generalization model to enhance prediction of earthquake-induced soil liquefaction," *Sensors*, vol. 22, no. 19, Article ID 7292, 2022.

[33] P. Aggarwal and S. K. Sharma, "Analysis of KDD dataset attributes—class wise for intrusion detection," *Procedia Computer Science*, vol. 57, pp. 842–851, 2015.

[34] N. V. Sharma and N. S. Yadav, "An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers," *Microprocessors and Microsystems*, vol. 85, Article ID 104293, 2021.

[35] L. Demarchi, A. Kania, W. Ciężkowski, H. Piórkowski, Z. Oświecimska-Piasko, and Jław Chormański, "Recursive feature elimination and random forest classification of natura 2000 grasslands in lowland river valleys of Poland based on airborne hyperspectral and LiDAR data fusion," *Remote Sensing*, vol. 12, no. 11, Article ID 1842, 2020.

[36] A. Srivastava, D. Sinha, and V. Kumar, "WCGAN-GP based synthetic attack data generation with GA based feature selection for IDS," *Computers & Security*, vol. 134, Article ID 103432, 2023.

[37] M. Mulyanto, J.-S. Leu, M. Faisal, and W. Yunanto, "Weight embedding autoencoder as feature representation learning in an intrusion detection systems," *Computers and Electrical Engineering*, vol. 111, Part A, Article ID 108949, 2023.

[38] A. Bibi, G. A. Sampedro, A. Almadhor, A. R. Javed, and T.-H. Kim, "Hypertuned lightweight and scalable LSTM model for hybrid network intrusion detection," *Technologies*, vol. 11, no. 5, Article ID 121, 2023.

[39] Y. Xiao, C. Kang, H. Yu, T. Fan, and H. Zhang, "Network traffic detection method based on an elevated Harris Hawks optimization method and gated recurrent unit classifier," *Sensors*, vol. 22, no. 19, Article ID 7548, 2022.

[40] P. R. Kanna and P. Santhi, "Hybrid intrusion detection using MapReduce based black widow optimized convolutional long short-term memory neural networks," *Expert Systems with Applications*, vol. 194, Article ID 116545, 2022.

[41] I. H. Hassan, M. Abdullahi, M. M. Aliyu, S. A. Yusuf, and A. Abdulrahim, "An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection," *Intelligent Systems with Applications*, vol. 16, Article ID 200114, 2022.

[42] H. S. Sharma, A. Sarkar, and M. M. Singh, "An efficient deep learning-based solution for network intrusion detection in wireless sensor network," *International Journal of System Assurance Engineering and Management*, vol. 14, pp. 2423–2446, 2023.

[43] E. H. Salman, M. A. Taher, Y. I. Hammadi, O. A. Mahmood, A. Muthanna, and A. Koucheryavy, "An anomaly intrusion detection for high-density internet of things wireless communication network based deep learning algorithms," *Sensors*, vol. 23, no. 1, Article ID 206, 2023.

[44] A. Thakkar and R. Lohiya, "Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system," *Information Fusion*, vol. 90, pp. 353–363, 2023.

[45] M. Bakro, R. R. Kumar, A. Alabrah et al., "An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier," *IEEE Access*, vol. 11, pp. 64228–64247, 2023.

[46] Y. Yang, Y. Gu, and Y. Yan, "Machine learning-based intrusion detection for rare-class network attacks," *Electronics*, vol. 12, no. 18, Article ID 3911, 2023.

[47] E. Mushtaq, A. Zameer, and R. Nasir, "Knacks of a hybrid anomaly detection model using deep auto-encoder driven gated recurrent unit," *Computer Networks*, vol. 226, Article ID 109681, 2023.

[48] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "A novel context-aware feature extraction method for convolutional neural network-based intrusion detection systems," *Neural Computing and Applications*, vol. 33, pp. 13647–13665, 2021.

[49] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder,"

IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6187–6196, 2021.

[50] W. Wei, Y. Chen, Q. Lin, J. Ji, K.-C. Wong, and J. Li, "Multi-objective evolving long–short term memory networks with attention for network intrusion detection," *Applied Soft Computing*, vol. 139, Article ID 110216, 2023.

[51] M. H. L. Louk and B. A. Tama, "Dual-IDS: a bagging-based gradient boosting decision tree model for network anomaly intrusion detection system," *Expert Systems with Applications*, vol. 213, Part B, Article ID 119030, 2023.