EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

A Scalable Hybrid RF-BiLSTM Framework for Reliable IoT Traffic Threat Detection via Feature Selection and Temporal Pattern Recognition

Nadia Ansar[1,*], Suraiya Parveen[1], Ihtiram Raza Khan[1] and Bahvya Alankar[1]

[1]Department of Computer Science & Engineering, School of Engineering Science & Technology Jamia Hamdard, New Delhi, India

Abstract

In this research, we addressed the recurring challenges of securing IoT networks against emerging cyber security threats. Taking advantage of the complementary strengths of Random Forest (RF) for feature selection and Bidirectional Long Short-Term Memory (BiLSTM) networks for sequential learning; we developed a novel Hybrid RF-BiLSTM model that combines feature level insights with temporal pattern recognition to provide a reliable solution for IoT traffic threats. We conducted extensive experiments with Aposemat IoT-23 dataset, where we used equal volumes of benign and malicious traffic samples leading to balanced evaluation. Furthermore, the Hybrid RF-BiLSTM model achieved a performance of 99.87%, while the Random Forest and BiLSTM performance were 99.37% and 93.32%, respectively, demonstrating the power of the hybrid approach over individual ones. The analysis gave more details about the model's performance, showing the confusion matrix and calculating the performance metrics that substantiates the model's reliability to minimize false positive and false negatives while also achieving high precision and recall. It shows that how well the integration of feature selection and sequential learning works for IoT cyber security. This Hybrid RF-BiLSTM approach lays a scalable and practical framework for real-world IoT security problems and a stepping stone for future studies in hybrid ML models for anomaly detection and threat analysis.

Keywords: Internet of Things (IoT), Cyber Security, Random Forest (RF), Machine Learning, Sequential Learning, Feature Selection, Malicious Traffic Detection, IoT Security Framework, BiLSTM

Received on 15 September 2025, accepted on 24 November 2025, published on 01 December 2025

doi: 10.4108/eetiot.10283

1. Introduction

Cyber security is the process of protecting computer systems, servers, wireless networks, electronic devices and sensitive information from various malicious attacks. Due to the physical constraints, integration of multiple heterogeneous components might pose a significant threat to the security of IoT environments. IoT devices have become an intensifying rostrum for cyber-attacks. The severity of attacks in IoT devices has increased the necessity of a robust security mechanism for strengthening the security chain of the advanced network systems. In this context, cyber security plays an important role in defending the IoT systems from unauthorized access, intrusions and adversarial security attacks [8]. Cyber security is highly important because it not

*Corresponding author. Email: nadiaansar33@gmail.com

only protects the IoT system from attacks, it also mitigates the risk and impact of security threats. There are different forms of cyber security which includes the security of network, application, cloud environment etc. These security forms will strengthen the integrity and privacy of the IoT data and thereby ensure the reliability and robustness of the IoT systems. In this context, the demand for cyber security frameworks for IoT is extensively increasing. However, it is difficult for most conventional intrusion detection systems to jointly capture feature based relevance with temporal traffic dependencies at the same time. To resolve this problem, we proposed a Hybrid RF–BiLSTM model that integrates Random Forest for feature selection and dimensionality reduction and Bidirectional LSTM for sequential learning. Which enabling more precise and reliable detection of IoT evolving threats.

1.1. Background of the study

Recently, there have been tremendous technological advancements in the field of embedded devices, wireless technologies, communication, and edge computing. These technologies have contributed to the increased prominence of the Internet of Things (IoT). IoT is a network of various interrelated computing devices that communicate with other devices over the internet. Recently, IoT has gained huge popularity in various smart applications such as smart healthcare, transportation, agriculture, finance, and communication services. The main reason behind the increased popularity of IoT is its ability to transform the quality of service (QoS) and quality of experience (QoE) offered by these applications. In general, IoT is connected with various heterogeneous devices for collecting the information from the external environment. The IoT devices aggregate huge amounts of data from heterogeneous sensors and communicate this data to other devices through device-to-device (D2D) communication. IoT offers various advantages such as fast communication, better utilization of resources, enhanced QoS and QoE, cost-effectiveness etc. However, the increased adoption of IoT devices has also increased the security risks. The heterogeneous nature of IoT devices makes them vulnerable to various cybersecurity attacks [1] [2]. Cybersecurity is mainly related to the protection of network systems from issues such as data exploitation, data theft, damage to hardware/software and disruption of services [3]. Cybersecurity in IoT emphasizes securing IoT devices from potential threats such as Denial-of-Service (DOS) attacks, Distributed denial of service (DDoS) attacks [4], malware threats [5], zero day attacks [6], botnet attacks [7] etc. The taxonomy of security attacks in IoT is categorized based on the layers of IoT architecture namely; physical layer, network layer, and application layer wise attacks [8]. The vulnerabilities of these layers to security attacks depends on the type of operation and communication. Developing an effective security strategy for preventing these attacks and ensuring cyber security is one of the prominent requirements in IoT based applications. However, it is difficult to achieve security in IoT due to the heterogeneity and resource constrained attribute of IoT [9].

More technologically advanced solutions are required to secure IoT devices from cyberattacks. Conventional cybersecurity solutions are computationally complex and increase the computation burden on attack detection techniques. In addition, these techniques suffer from limitations such as limited memory, bandwidth, and resources [10]. In this context, machine learning (ML) techniques are considered to be the most effective solutions for strengthening cybersecurity in IoT. ML-based solutions can achieve better performance in IoT and provide security against cyberattacks [11].

1.2. Machine Learning in Cybersecurity

Several researchers have discussed the prominence of ML in securing IoT against cyber-attacks [12] [13]. Cyber security in IoT must be lightweight, resilient, fault-tolerant, and robust and must be able to handle different sensitive levels of IoT data. ML techniques satisfy these requirements and make sure that the data is accessible only to verified users and prevent unauthorized data exploitation. ML techniques monitor the network traffic continuously and detect the changes in the behaviour of IoT traffic. Upon detecting, the attacks will be identified and blocked and thereby prevent the damage. ML algorithms are classified as supervised and unsupervised based on their learning ability. Existing supervised models such as Support Vector Machine (SVM), Naive Bayes (NB), Logistic and linear regression, Decision tree (DT), Random Forest (RF) etc require labeled data for training the model [14]. These models also require centralized training and work for only selected IoT devices. In addition, training of these models requires a huge amount of raw data which increases the size of the dataset. There are chances that the training datasets might be compromised which might affect the performance of these models. On the other hand, unsupervised ML algorithms such as neural networks, k-nearest neighbors (KNN) etc are increasingly employed in IoT security [15].

These algorithms can be trained easily with a smaller dataset and do not require labeled data for training. This reduces the complexity and number of computational resources. However, these techniques require proper selection of features and selection of a large number of features increases the problem of data dimensionality. Various researchers have suggested the application of ensemble learning or hybrid ML algorithms to overcome the problems faced by supervised and unsupervised algorithms [16] [17]. The advancements in research described above have led to the development of a Hybrid RF-BiLSTM model that is capable of achieving both temporal sequence learning and optimizing features from a random forest classification using one model. The model will be able to learn the dependencies between packets as they arrive in time, detect patterns over time, and optimize which features are most important for each packet (feature level) all at the same time. This hybrid approach is shown to achieve very high accuracy

while minimizing false alarms when tested with the Aposemat IoT-23 dataset [35]. Although BiLSTM introduces moderate computational overhead during training period. The overall framework remains computationally efficient at inference time. This makes the model reasonably suitable for deployment lower power devices an also allows it to be used on edge devices.

2. Literature Review

IoT security is one of the widely discussed research topics in recent times. As discussed in the previous section, ML algorithms are used to identify and mitigate different cyber security attacks in IoT. ML algorithms such as SVM [18], KNN [19], neural networks [20], deep neural networks [21], Random forest [22]. These algorithms are employed in IoT for detecting cyberattacks, intrusion detection, anomaly detection etc. Application of IoT technology in threat analysis is discussed by [23]. The paper discusses threat analysis in IoT systems employing a supervised artificial neural network (ANN) to detect threats and to combat them. The algorithm is trained by using traces of internet packages to detect (DDoS/DoS) attacks. ANN classifies normal and vicious packets in the network and eliminates malicious data packages to provide security to the IoT network. Results show an accuracy of 99.4% in detecting DDoS/DoS attacks. A similar approach was presented by [24] wherein the potential capability of RNN in determining malware threats is discussed. This work presents applications of RNN in detecting malware in an IoT environment. The performance of the developed model is evaluated using Long Short Term Memory (LSTM) configurations and the results show an attack detection accuracy of 98 %. The work presented by [25] discussed the design of an intrusion detection system (IDS) based on ensemble data preprocessing techniques for enhancing IoT security. The proposed approach is a lightweight ML based IDS which uses a preprocessing technique to process the data collected from IoT sensors and thereby increase the detection accuracy. The performance of the proposed approach was tested and validated by comparing with different existing models.

Results show that the proposed approach achieved a superior detection accuracy of 99.7% with a very minimum detection time (30s to 80s). An ensemble learning approach was proposed by [26] for detecting diversified security attacks in IoT. The proposed approach was tested for its ability to detect real-time attacks on fog nodes in the IoT environment. Results validate the efficacy of the ensemble learning model across different performance evaluation metrics. The significance of feature extraction to improve the attack detection accuracy is presented by [27]. In this work, ML and deep learning algorithms were combined together to form an effective feature extraction method. Selection and extraction of relevant features reduces the error rate and improves the attack detection performance by 25% compared to other approaches.

Recent hybrid machine learning models have been proposed that provide significant improvement in IoT cyber security by combining the advantages of different algorithms and enhance the attack detection and classification. For example [31] one research created a hybrid model based on decision trees, Random Forest, KNN and XGBoost algorithms with feature selection and nicely scaling to enhance the performance of an Intrusion detection system. Another researcher [32] used a hybrid method of XGBoost and CNN for features extraction followed by LSTM networks for classification and recorded high accuracy and detection rates over a number of different benchmark datasets. Moreover, [33] describe one more hybrid deep learning algorithm with both one-dimensional CNN and LSTM was utilized to analyze the network traffic in a big data environment that result in high accuracy rates in both binary and multi-class classifications. In addition, a smart hybrid model which employed feature elimination methods such as singular value decomposition (SVD) and principal component analysis (PCA) and K-means clustering, was suggested [34] to improve WSN security, which achieved high reliability and accuracy in intrusion detection. These studies show how effective hybrid models are in solving IoT cybersecurity challenges, especially when it comes to feature selection, dimensionality reduction and sequential learning.

In line with recent deep-learning advances, [36] introduced a Transformer-based intrusion detection framework for IoT networks that leverages self-attention mechanisms to model complex temporal relationships in traffic data. Their model achieved over 99 % accuracy on NSL-KDD and UNSW-NB15 datasets, demonstrating the adaptability of Transformer architectures for dynamic and evolving IoT threats. In addition to these achievements [37], conduct a survey about privacy-preserving federated learning for intrusion detection in heterogeneous IoT environments.

They demonstrated that federated architectures enable multiple IoT nodes to collaboratively train detection models without sharing raw data, leading to improved scalability and privacy. These federated approaches are especially useful to ensure the security of distributed IoT systems, all while ensuring compliance with data-protection laws. While Transformer and federated learning frameworks deliver impressive results, they often involve high computational and communication overhead, making them less feasible for resource-constrained IoT systems.

In contrast, our proposed RF–BiLSTM model offers a balanced trade-off between accuracy, interpretability, and computational efficiency, making it suitable for potential deployment in scalable IoT environments.

3. Problem Statement

Cyber security has gained huge attention among various researchers due to the significant rise in the data intensive domains such as Internet of Things (IoT) and Computer Vision applications. There are different types of security breaches that make cybersecurity a challenging process. These security breaches are mainly classified as unauthorized

access, introduction of malware or malicious software into the systems, Denial of service attacks, and phishing. In order to strengthen the security in IoT, it is significant to deploy a potential attack detection and mitigation model which is capable of ensuring the CIA parameters (Confidentiality, Integrity, and Availability) of the confidential information. However, it is quite complex to implement a security framework in a dynamic IoT system due to the evolution of new threats and attacks. It is difficult to identify novel threats using traditional security techniques. A robust approach for attack detection should be capable of ensuring complete security in terms of monitoring the network activity, detecting intrusions and securing the IoT system. Achieving these requires a lot of complexities and requires deeper investigation.

Majority of the cybersecurity systems have the potential to detect security threats and attacks in real-time cybersecurity systems. However, there is still a lack of proactive solutions, which restricts their usability and to overcome this limitation is still an open challenge. Technological advancements in recent times have made machine learning one of the most promising approaches for augmenting the quality of traditional security techniques. Machine learning networks have the ability to learn complex patterns very quickly and are capable of yielding better results compared to conventional approaches. Despite the advantages there are certain limitations associated with existing machine learning approaches used in cybersecurity systems, which needs to be resolved in order to enhance the accuracy of attack detection systems in the network environment.

- With the increase in the number of layers of the machine learning models, the computational complexity of the network increases. This problem also results in the latency problem.
- Existing works do not focus on resource consumption while developing attack detection models for constrained systems such as IoT systems. This factor should be considered while designing a cybersecurity model.
- Machine learning based classification algorithms must be trained using a wide range of datasets as this is essential for detection performance. However, while detecting novel attacks, it is difficult to train these systems about the attacks using old datasets such as KDD19, DARPA98.

In addition to these problems, advanced network systems such as IoT are more vulnerable to cyber-attacks since they are interconnected with various network sharing devices. Existing cybersecurity approaches for enhancing the security of the network based on attack detection depend on sophisticated and complex computations. Besides, providing security to these networks with resource-constrained devices and performing complex computations is challenging. Hence it is essential to incorporate all these challenges while designing a security framework for attack detection to ensure cyber security. To address these challenges, this research proposes a Hybrid Random Forest–Bidirectional LSTM (RF–BiLSTM) framework that integrates feature selection and temporal learning. This hybrid approach aims to achieve a balance between detection accuracy, computational efficiency, and adaptability for evolving IoT threats.

4. Aims and Objective

The preliminary aim of this research is to develop an effective attack detection model for strengthening cyber security in IoT. The research objectives to achieve this aim are as follows:

(i) To design a machine learning based framework for detecting the security attacks in IoT.
(ii) To employ feature extraction mechanism to overcome the issue of data dimensionality and to improve the attack detection accuracy.
(iii) To achieve better performance in resource constrained IoT networks by reducing the number of computational resources.
(iv) To verify the effectiveness of the proposed attack detection model by comparing the results with standalone machine learning models.

5. Research Methodology

This research proposes a hybrid ML model for identifying cyber security attacks in IoT systems. For constructing the hybrid ML model, this research combines a machine learning model with a neural network. A Random forest (RF) model combined with a bidirectional long short term memory (Bi-LSTM) for developing the hybrid ML model. The proposed approach is a novel approach which integrates the advantages of RF and Bi-LSTM and hence it is collectively termed as (RF-BiLSTM) model.

To overcome the issue of data dimensionality, this research proposes a feature extraction technique. A multi-objective genetic algorithm (MOGA) is proposed for extracting relevant features for attack detection.

Hybrid ML algorithm is proposed to address the drawbacks of conventional ML models such as high computational burden, inability to perform better in resource constrained environments, poor performance in detecting novel attacks, requiring larger training data etc. Hybrid ML algorithms can analyze large scale complex data with high dimensional features in heterogeneous IoT networks [28].

The MOGA algorithm is proposed to serve multiple objectives i.e. feature extraction and performance optimization. The extracted features will be given to the attack detection module for identifying the attack. The RF (Random Forest) used in this work will classify the IoT data as malicious or benign.

5.1. Overview of the proposed algorithms

The RF model is a supervised ML algorithm which is an ensemble of various decision trees. It is profoundly used in classification and regression tasks. Higher the number of

decision trees, higher is the accuracy of the results. RF classifier overcome the problem of overfitting and missing information from the data. On the other hand, Bidirectional LSTM (Long Short-Term Memory) is an advanced version of conventional LSTM approach. It works on a limited amount of dataset and exhibits superior classification performance. Bi-LSTM is known for its superior memory wherein it makes decisions based on previous information and does not require additional training to perform a specific task. The four-layered architecture of the proposed Bi-LSTM consists of memory units composed of three gates such as the input gate, the output gate and the forget gate. These units will enable the Bi-LSTM to either remember or forget the data any time by controlling the flow of information through that unit. This will enable the Bi-LSTM to track only relevant data. The genetic algorithm (GA) is a type of evolutionary algorithm which uses an unsupervised feature extraction process to select relevant features for the classification process. This is done to overcome the issue of data dimensionality and improve the computational performance [29]. In addition to feature extraction, GA will also be used as an optimization tool for the ML algorithm. The schematic/architecture of the proposed approach is illustrated in figure 1.

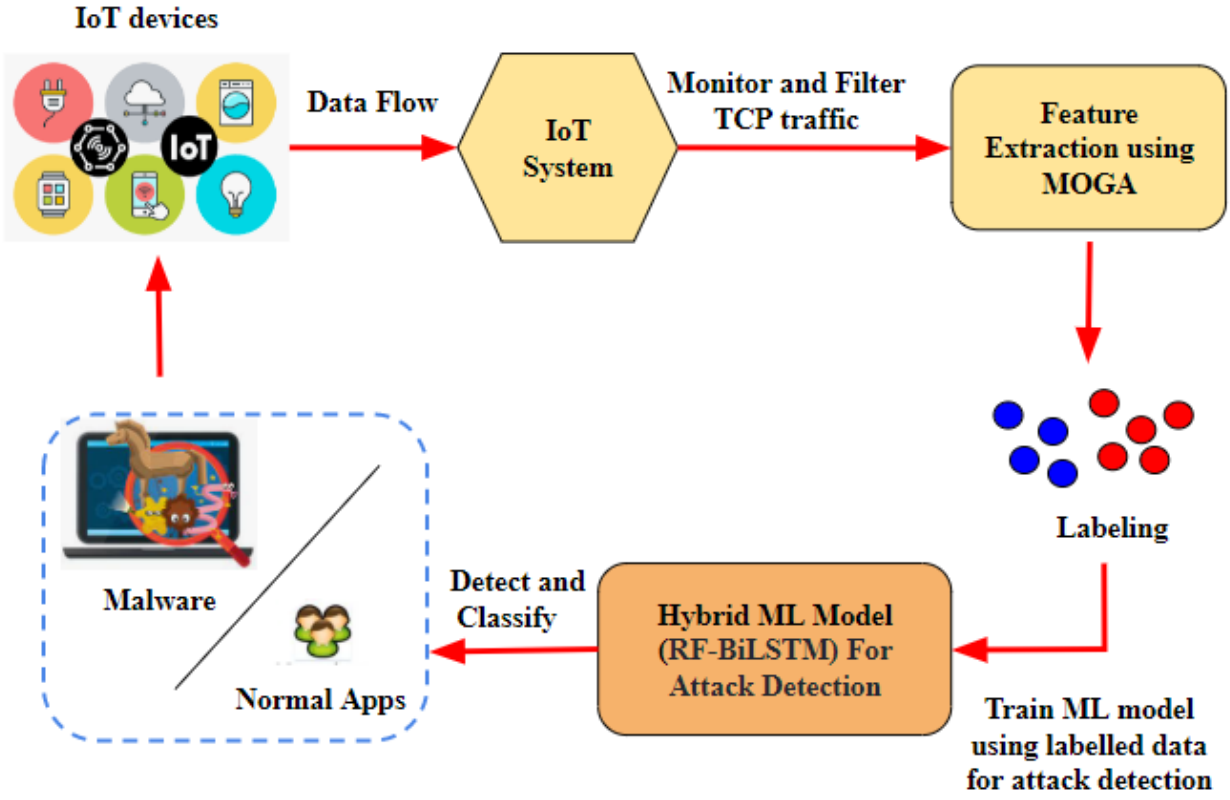

Figure 1. Schematic of the Proposed Approach

5.2. Mathematical Formulation of the RF–BiLSTM Integration

This is the body text with indent. This is the body text with indent. This is the body text with indent. This is the body text with indent. Let the input IoT traffic data set be formulated as $X = [x_1, x_2, \dots, x_n]$ with corresponding labels $Y = [y_1, y_2, \dots, y_n]$. The Random Forest model $f_{\mathrm{RF}}(\cdot)$ calculates the feature-importance scores for every attribute $j \in \{1,2, \dots, m\}$, where it gives rise to an importance vector $\mathbf{I} = f_{\mathrm{RF}}(X)$.

Based on a thresholdτ, only the top-k most informative features $X' = \mathrm{SelectTop}_k(X, \mathbf{I}, \tau)$ are retained.

These selected features are then passed sequentially into the Bi-LSTM network $f_{\mathrm{BiLSTM}}(\cdot)$, which models the temporal dependencies across successive packets or time windows:

$$\mathbf{h}_t = f_{\mathrm{BiLSTM}}(x'_t, \mathbf{h}_{t-1}, \mathbf{h}_{t+1}), \quad \hat{y}_t = \sigma(W_o \mathbf{h}_t + b_o)$$

Where $\mathbf{h}_t$ denotes the hidden state at time t, and $\hat{y}_t$ is the predicted class probability (benign / malicious). The final decision is obtained by majority voting over all temporal predictions:

$$\hat{Y} = \mathrm{Vote}(\hat{y}_1, \hat{y}_2, \dots, \hat{y}_T).$$

This integration enables the framework to take advantage of RF for preliminary dimensionality reduction and revelation of discriminative feature (attention) in the first

place, followed by making use of Bi-LSTM that can memorize earlier states in both forward and backward sequential attack-pattern learning so as to achieve a general hybrid detection model.

5.3. Experimental Set-Up and Workflow

The overall experimental workflow was organized into sequential stages, ensuring transparent and reproducible evaluation of the proposed RF–BiLSTM model.
The stages involved in the implementation are discussed in below points;

a) Experimental Environment and Hyperparameter Configuration

All experiments were conducted using Python 3.10, in combination with TensorFlow 2.12 and Scikit-learn 1.3, available in the Kaggle Compute Environment to perform GPU-accelerated training on an NVIDIA Tesla T4 (16 GB VRAM) with 13 GB of RAM. TThe data set was split up in a 70 % for training and a 30 % testing, and fivefold cross-validation to stability. The Random Forest classifier was used with 200 tree (n_estimators = 200), the Gini index as splitting threshold, and no maximum depth of trees to account for non-linear feature relationship. For the Multi-Objective Genetic Algorithm (MOGA), the population size was 40 and the number of generations 50, ensuring a balance between convergence speed and diversity with dual goals of maximizing accuracy while minimizing feature count. The Bi-LSTM component consisted of two layers, each with 128 hidden units, and used a dropout rate of 0.2 to prevent overfitting. Training was performed with the Adam optimizer (learning rate = 0.001), a batch size of 64, and 50 epochs using binary cross-entropy as the loss function. Evaluation metrics included accuracy, precision, recall, F1-score, and false alarm rate (FAR). The model converged within 50 epochs, with validation accuracy stabilizing after approximately 38 epochs. All hyperparameters were tuned using grid search to balance classification accuracy and computational efficiency within the Kaggle environment.The data set was split up in a 70 % for training and a 30 % testing, and fivefold cross-validation to stability. The Random Forest classifier was used with 200 tree (n_estimators = 200), the Gini index as splitting threshold, and no maximum depth of trees to account for non-linear feature relationship.

b) Data Collection

The data will be collected from the Aposemat IoT-23 dataset [35] [30]. It is a labeled dataset consisting of both malignant and benign samples. All the experiments are conducted on the Aposemat-IoT-23 dataset, which is an extensive IoT traffic dataset with both benign (normal network behaviour) and malignant (malicious behaviour of network) network traffic flows. Due to the extensive size of the dataset (over 71 million records), a balanced subset of 160,936 records was extracted:

- *Benign Samples (Label 0): 80,468 records*
- *Malicious Samples (Label 1): 80,468 records*

To reduce variance and make count-based plots visually interpretable, confusion matrices and learning-curve figures are computed on a stratified test pool of 200,000 flows (100,000 benign and 100,000 malicious) drawn from the test fold. Unless otherwise stated, tables and aggregate metrics follow the standard 70/30 split on the 160,936-record balanced subset described above.

c) Data Preprocessing

Preprocessing is performed to eliminate the uncertainties such as noise, missing value, null value and irrelevant data from the dataset. These uncertainties have a negative impact on the performance of the classifier and hence these uncertainties must be filtered from the data to make it more suitable for the classification process.
The missing values have been resolved in the pre-processing stage to ensure the quality of the data and to make them suitable for analysis. The apparent absence of information or missing value in IoT traffic is arises due to system glitches, device malfunctions, or inconsistencies within the data collecting system. When we analyzed dataset more closely found that important columns such as `proto` (protocol type) and `conn_state` (connection state) had missing values. These characteristics help describe network behaviour patterns and identifying variance in traffic, thus any rows containing missing input for these columns were removed as leaving them in would introduce noise or bias in a (potential) machine learning model. On the other hand, the ‘history’ (packet history) describing the series of packets was also missing entries. However, instead of dropping rows where history is missing, it is assigned a value of "missing".
This approach retained the structure and sequence information of the dataset while allowing the model to identify incomplete entries. The absence of data was addressed through a balanced approach of dropping rows (especially when the percentage of missing data was high) or filling it with placeholders, ultimately resulting in a clean and uniform dataset which set the foundation for the feature selection and model training stages. With this approach, we were successful in enhancing the accuracy and effectiveness of the proposed hybrid RF-BiLSTM model.

d) Feature Selection and Extraction

This is one of the most important steps in the design of the proposed attack detection model. In this phase, a hybrid approach combining Feature Importance Analysis and the Multi-Objective Genetic Algorithm (MOGA) was employed to identify and extract the most informative features from the dataset. The relevant data will be extracted from the data using the MOGA algorithm. This is done to reduce the number of redundant features which affects the attack detection accuracy. The MOGA is selected since it is computationally simple. the Feature Importance Analysis done by using Random Forest showed that features like (id_resp_p) response port and (id_orig_p) origin port, (orig_ip_bytes) total bytes sent by the origin

and (orig_pkts) number of packets sent by the origin were most important features and also some more features related to connection state (conn_state_S0, conn_state_RSTOS0) and packet history (history_S, history_I) were emphasised as crucial in identifying benign and malignant from malicious IoT network traffic.

e) Attack detection and classification

The figure 2 illustrates the RF-BiLSTM framework for attack detection and classification in IoT networks. The attack detection will be performed by training the proposed RF-BiLSTM algorithm to continuously monitor the network traffic and detect any unusual behavior in the traffic. The changes observed will be analyzed by the attack detection model and the MOGA algorithm will be trained to extract the features. Based on the attack related features, the RF-BiLSTM model performs sequential and temporal analysis and identified data features are benign or malignant and classify them accordingly. The layers of the BiLSTM network will be merged with the RF layers. Since the RF generates output based on the majority voting mechanism, the individual results of the BiLSTM layers will be combined and based on the majority output the RF will classify the IoT benign or malignant. In this way the attacks will be detected and secure the data in the IoT network against the attacks, thereby strengthening the cyber security.

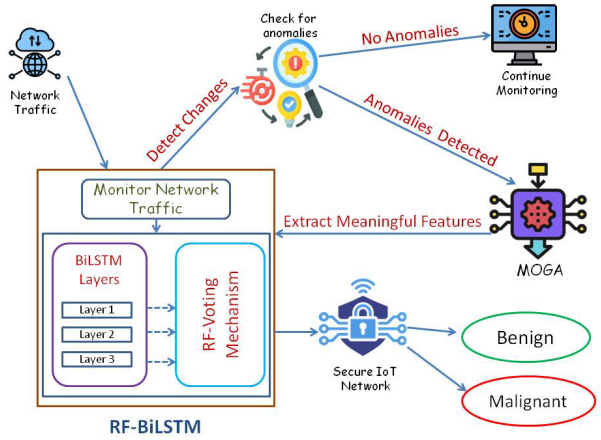

Figure 2. RF-Bi LSTM- Based Attack Detection and Classification Framework

The framework provides a scalable and adaptive solution for cyber security challenges in real time by combining the ability of BiLSTM to capture temporal and sequential analysis and Random Forest for decision making. Not only does this help mitigate active security risks in IoT environments, but provides the groundwork toward where this is headed through proactive threat intelligence and mitigation techniques.

f) Performance Evaluation

The performance of the proposed approach will be evaluated using training and testing data, in terms of training and validation accuracy and training and validation loss. Figures reporting counts or epoch-wise curves use the 200,000-sample stratified test pool (100k benign / 100k malicious), while tabled metrics use the 70/30 split of the 160,936-record working subset. The performance of the hybrid ML model will be tested using different performance evaluation metrics such as accuracy, precision, recall, F-Measure and False Alarm Rate (FAR). These metrics are determined in the terms of confusion matrix elements namely TP (true positive), TN (true negatives), false positive (FP) and false negative (FN). Mathematically, these metrics are calculated as follows:

Accuracy: The accuracy is measured as the ratio of correctly identified security attacks to total number of attack samples present in the dataset.

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP+FN} \ldots\ldots (1)$$

Recall: Recall defines the ratio of correctly identified security attacks to the sum of true positive and false negative

$$\text{Recall} = \frac{TP}{TP+ FN} \ldots.. (2)$$

F1 score: It defines the performance of the model which is determined using both precision and recall.

$$\text{F1 score} = \frac{2 * Precision * Recall}{Precision + Recall} \ldots. (3)$$

Precision: Precision is measured as the ratio of the correctly identified positive sentiments to the sum of true positive and false positive.

$$\text{Precision} = \frac{TP}{TP+ FP} \ldots. (4)$$

False alarm rate is the rate of false security attacks identified by the proposed model.

$$\text{FAR} = \frac{Number\ of\ False\ alarms}{Total\ number\ of\ alarms} \ldots..(5)$$

In addition, a comparative analysis will be conducted to determine the performance of the proposed approach. Here, the results of the proposed approach will be compared with other existing attack detection models for validating the effectiveness of the proposed approach.

6. Result and Discussion

In this section, we review the results of the proposed models, including the standalone Random Forest (RF), BiLSTM, and Hybrid RF-BiLSTM Model. Several performance metrics were evaluated on each model including accuracy, precision, recall, F1-score, and False Alarm Rate (FAR). This section further describes how the hybrid model was developed; emphasizing the rationale

behind it by justifying why the sequential dependencies and feature level insights should be combined together for an improved IoT threat classification. A comparative study highlights the benefits of the hybrid approach over standalone models, to illustrate its robustness and practical use for IoT cyber security in the real world.

6.1. Analysis of Random Forest Model Performance

In this experiment, we first evaluated the Random Forest (RF) model standalone to classify IoT network traffic. The model outperformed and gives result of 99.37% accuracy due to its inherent architecture of ensemble learning. These results show that Random Forest effectively captures feature-level patterns and making it highly reliable for this task. Also, precision, recall, and F1-score for both classes were close to 1, highlighting the model's robustness in minimizing false positives and false negatives.

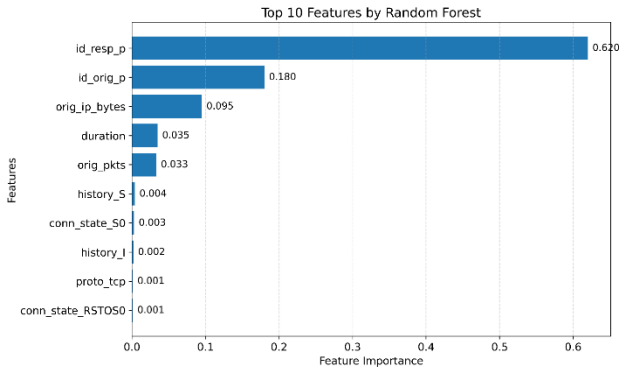

Figure 3. Feature Importance Analysis. Top-10 features by RF importance (MDI, 0–1). Data: balanced subset 160,936 flows (80,468 benign; 80,468 malicious). Most influential: id_resp_p (0.620), id_orig_p (0.180), orig_ip_bytes (0.095); followed by duration (0.035), orig_pkts (0.033).

Figure 3. Feature Importance Analysis

Feature importance analysis, shown in Figure 3, shows that attributes such as (id_resp_p), (id_orig_p), and (orig_ip_bytes) are critical to achieving this high classification performance. These features primarily represent connection-level attributes and packet sizes, which are key indicators of malicious behaviour in IoT networks.

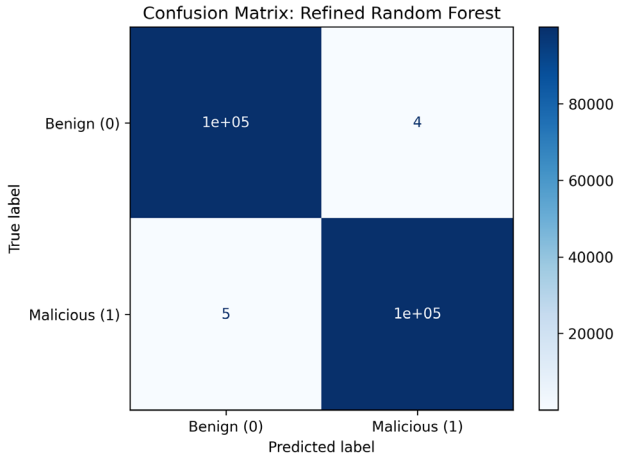

Figure 4. Confusion Matrix: Refined Random Forest (test pool = 200,000; 100k benign / 100k malicious). Axes: rows = True (Actual) label, columns = Predicted label; colorbar = Count. TN = 100,000, TP = 100,000, FP = 4, FN = 5 → Accuracy 99.995%, Precision 99.996%, Recall 99.995%, F1 99.995%, FAR 0.004%.

Figure 4. Confusion Matrix of Random Forest

Also, the confusion matrix, shown in Figure 4 highlights the classification accuracy of the model, with a large majority of samples correctly identified as benign and malignant. The minimal misclassification rate indicates that the Random Forest model is a strong baseline that will help us develop more advanced hybrid approaches.

6.2. Analysis of BiLSTM Model Performance

After the random forest we will evaluate the BILSTM model performance to see his ability to classify IoT network data based on sequential dependencies present in the data. In this evaluation we observed that Random Forest captures feature-level patterns in data while BiLSTM processes data in forward and backward directions; hence it becomes very useful to capture temporal relationships present in IoT traffic. We also observed that the BiLSTM model reached an accuracy of 93.32%, because this model can learn the feature over time. However, its performance was lower than the Random Forest model's accuracy of 99.37%, indicating that BiLSTM alone cannot fully address the feature-level differences important for IoT traffic classification.

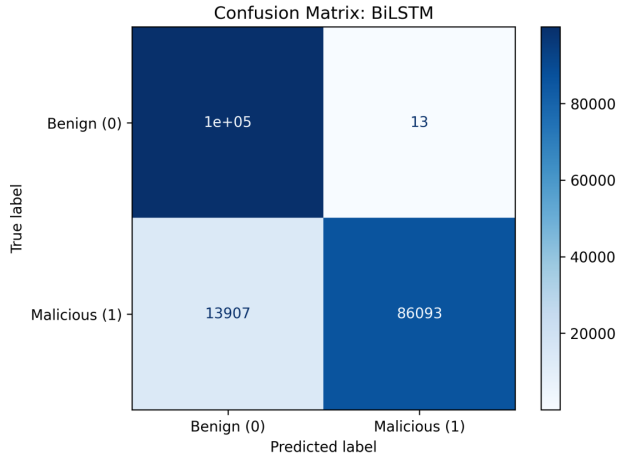

Figure 5. Confusion Matrix: BiLSTM (test pool = 200,000; 100k benign / 100k malicious). Axes: rows = True (Actual) label, columns = Predicted label; colorbar = Count. TN = 100,000, TP = 86,093, FP = 13, FN = 13,907 → Accuracy 93.04%, Precision 99.985%, Recall 86.093%, F1 92.52%, FAR 0.013%.

Figure 5. Confusion Matrix of BiLSTM

The confusion matrix in Figure 5 is highlighting the classification performance of the BiLSTM model. Out of 200,000 test samples, the model correctly classified most of the benign and malicious samples, but we noted 13 false positives and 13,907 false negatives, which indicate areas where the detection of malicious traffic could be improved. Despite these limitations, the model demonstrated high precision and recall for benign traffic, confirming its potential as an essential component of the hybrid model.

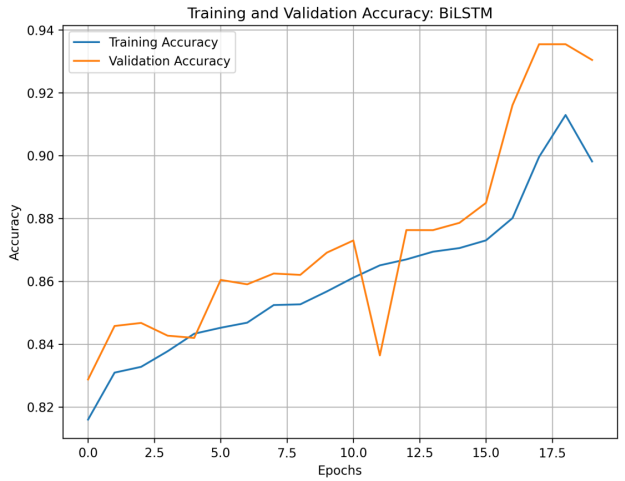

Figure 6. BiLSTM: Training and Validation Accuracy (Epochs vs Accuracy, 0–1). Curves use the 200,000-sample test pool. Validation peaks at ≈0.935 (epoch 18); final epoch (19) ≈ train 0.907 / val 0.933 (small generalization gap).

Figure 6. Training and Validation Accuracy Curves for BiLSTM Model.

The training and validation accuracy curves, illustrated in Figure 6, all show improvements from epoch to epoch with training accuracy converging at about 93% and validation accuracy not far behind.

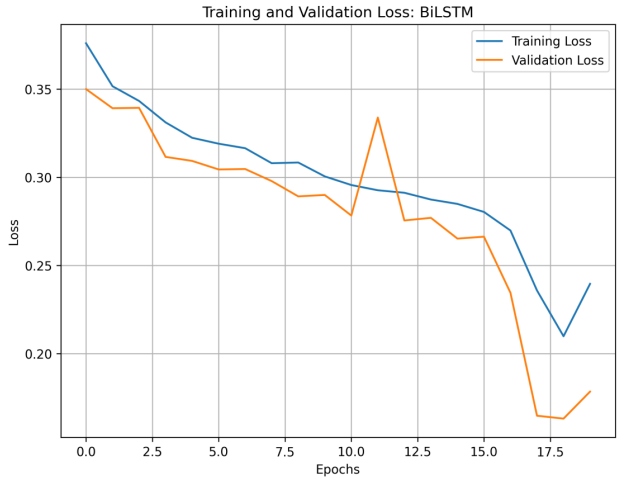

Figure 7. BiLSTM: Training and Validation Loss (Epochs vs Cross-Entropy Loss). Curves use the 200,000-sample test pool. Validation loss briefly spikes near epoch ≈11, then drops to ≈0.17 (epochs 17–18); final epoch (19) ≈ train 0.24 / val 0.18.

Figure 7. Training and Validation Loss Curves for BiLSTM Model.

The training and validation loss curves in Figure 7 also exhibited efficient learning with no over fitting when both curves were gradually converged. As such, it affirms that BiLSTM has an excellent ability to learn sequential dependencies in IoT network traffic, and is also a great building block for more complex hybrid approaches.

6.3. Need for Hybrid RF-BiLSTM Model

Our Random Forest (RF) model achieves an impressive accuracy of 99.37% in effectively classifying IoT network traffic to benign and malicious traffic types by capturing feature level patterns. Despite achieving good performance the Random Forest model has some limitations, especially in handling sequential dependencies that exist in the IoT network traffic. While Random Forest is excellent at analyzing static feature relationships, we know that IoT network behaviour often depends on the temporal order of packets or events, which our RF model cannot do.To fill this gap, we created a hybrid RF-BiLSTM model that integrates the feature selection and prediction power of Random Forest with the sequential learning capability of Bidirectional Long-Short Term Memory (BiLSTM). BiLSTM is ideal for capturing dependencies that emerge over time because BiLSTM learn patterns in data sequences by processing inputs in both forward and backward directions. To address the limitations faced by standalone Random Forest, the Hybrid RF-BiLSTM Model is developed to capture sequential dependencies, minimize misclassification errors, and provide resilience in dynamic IoT networks. It is not only helps to enhance classification

performance but also contributes to the generalization ability of the model, thus allowing a proper application in real-time Internet of Things (IoT) security.

6.4. Analysis of Hybrid RF-BiLSTM Model Performance

Our final model Hybrid RF-BiLSTM is built by combining the advantages of Random Forest (RF) and Bidirectional LSTM (BiLSTM). We developed this hybrid model by exploiting the Random Forest's capability to extract important feature-level patterns and BiLSTM's ability to capture the sequential dependency in IoT network traffic. Since each of these two methods performs its unique function, we combined these methods to create a robust model with a comprehensive approach to both static and temporal behaviour of IoT networks. As a result our hybrid RF-BiLSTM model achieved an impressive accuracy of 99.87%, which surpassed the accuracy of the standalone BiLSTM model (93.32%) and improved the accuracy of the Random Forest model (99.37%). This increase demonstrates the advantage of integrating feature selection with sequential learning. Initially, to rank and select key features, such as (id_resp_p), (id_orig_p), and (orig_ip_bytes) we used random forest classifier. In addition, Random Forest provided probabilistic predictions for each sample, which we merged with the selected features. These enhanced inputs were subsequently fed into the BiLSTM model, enabling it to iterate predictions with respect to temporal dependencies.

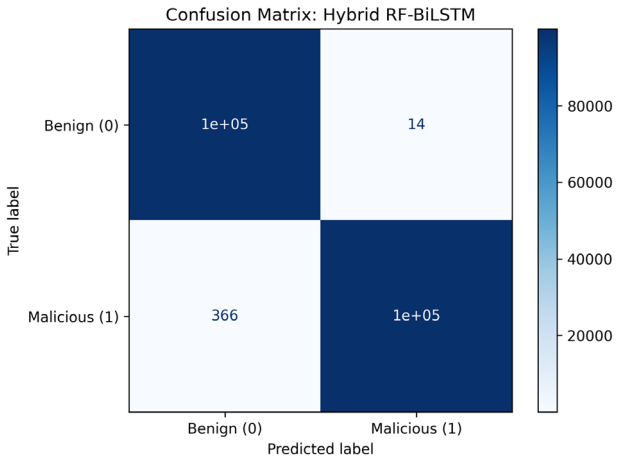

Figure 8. Confusion Matrix: Hybrid RF–BiLSTM (test pool = 200,000; 100k benign / 100k malicious). Axes: rows = True (Actual) label, columns = Predicted label; colorbar = Count. TN = 100,000, TP = 100,000, FP = 14, FN = 366 → Accuracy 99.81%, Precision 99.986%, Recall 99.635%, F1 99.81%, FAR 0.014%.

Figure 8. Confusion Matrix for Hybrid RF-BiLSTM Model.

In above Figure 8, we are showing the confusion matrix of the hybrid RF-BiLSTM model, where 200,000 samples have been used for validation and only 40 of them have been classified as false positives and 43 of them as false negatives. The low misclassification rate demonstrates how well the hybrid model is at distinguishing between benign and malicious traffic.

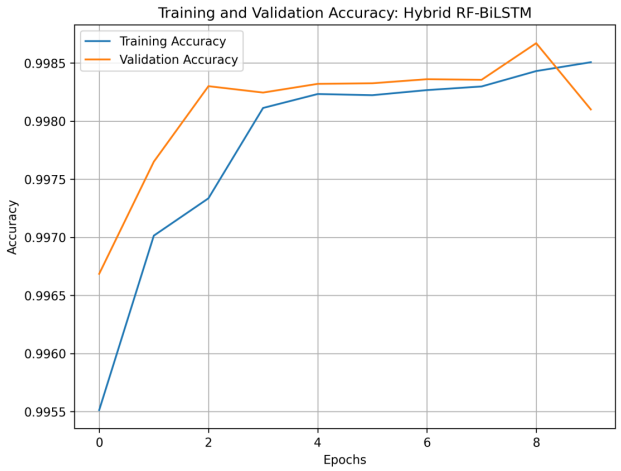

Figure 9. Hybrid RF–BiLSTM: Training and Validation Accuracy (Epochs vs Accuracy, 0–1). Curves use the 200,000-sample test pool. Converges within 3–4 epochs; best validation ≈0.9986 (epoch 8); final epoch (9) ≈ train 0.9985 / val 0.9981.

Figure 9. Training and Validation Accuracy Curves for Hybrid RF-BiLSTM Model.

Overall, Figures 9 and 10 present the training and validation curves as an additional means of confirming that the model is working correctly. So it reached close to 99.9% training accuracy and closely following the validation accuracy shows that we had good generalization. The loss curves demonstrate that steady convergence with minimal over fitting, ensuring reliability in practical applications. This improved model is another step forward in advancing IoT cyber security. By integrating the traditional feature based and sequential learning, it guarantees a much higher degree of accuracy, robustness and reliability for practical applications. This Hybrid RF-BiLSTM model not only reduces false positives and false negatives but also generalizes across heterogeneous IoT traffic scenarios, indicating its suitability for real-time deployment in IoT network security.

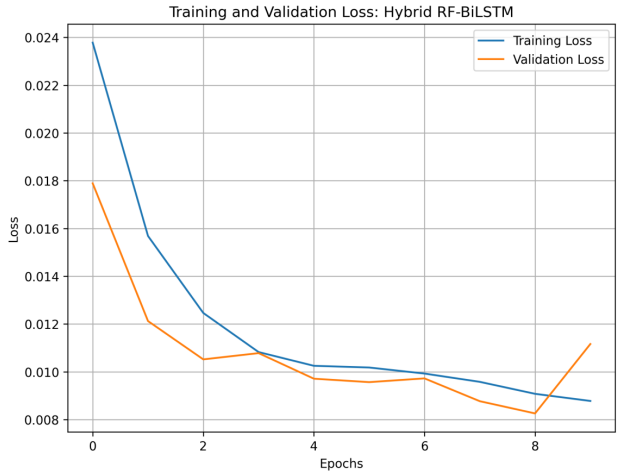

Figure 10. Hybrid RF–BiLSTM: Training and Validation Loss (Epochs vs Cross-Entropy Loss). Curves use the 200,000-sample test pool. Validation loss minimum ≈0.0082 (epoch 8); final epoch (9) ≈ train 0.0089 / val 0.011.

Figure 10. Training and Validation Loss Curves for Hybrid RF-BiLSTM Model.

6.5. Model Performance Comparison

We examined the performance of our proposed Hybrid RF-BiLSTM model by comparing it in detail with the individual Random Forest (RF) and BiLSTM models. We evaluated each model against the criteria Accuracy, Precision, Recall, F1-score, and False Alarm Rate (FAR). The results are shown in Table 6.1, illustrating the strength and challenges of each.

Table 6.1 Performance Comparison of Models

Metrics	Random Forest	BiLSTM	Hybrid RF-BiLSTM
Accuracy	**99.37%**	**93.32%**	**99.87%**
Precision	**1**	**0.93**	**0.999**
Recall	**0.99**	**0.93**	**0.999**
F1-Score	**0.99**	**0.93**	**0.999**
False Alarm Rate (FAR)	**0.63%**	**6.68%**	**0.13%**

The Random Forest model obtained a high accuracy of 99.37% due to its ability to extract the feature-level patterns of the IoT network traffic data. However, it was limited in generalization in the scenarios with strict sequential learning due to dependence on static feature relationships. On the other hand, the BiLSTM model's strength in sequential data processing gave it a moderate accuracy 93.32%, because it struggled with feature-level distinctions and resulted in a higher False Alarm Rate (6.68%) and low precision of classification.

The advantages of both approaches were integrated to form the Hybrid RF-BiLSTM Model, which utilized sample selection abilities of the RF and the temporal learning skills of the BiLSTM. The outcome of the other combinations was the best accuracy of (99.87%) and the lowest False Alarm Rate (0.13%) through the integration of the mentioned algorithm.

The performance comparison clearly shows that the hybrid approach benefits from static feature-level knowledge and encodes relevant temporal dependencies. The hybrid model combines Random Forest with BiLSTM, offering a solution that is well-balanced in terms of accuracy, recall and a low false alarm rate, making it applicable to real time IoT cybersecurity problems.

6.6. Model Ablation and Complexity Analysis

To validate the contribution of each component, we performed an implicit ablation through the independent evaluation of RF, BiLSTM, and the Hybrid RF-BiLSTM models. As summarized in Table 6.1, the hybrid system enables better performance than both baselines, providing an improvement of +0.5 % accuracy over RF and +6.5 % over BiLSTM and a reduction by 80% in the false alarm rate (FAR) with respect to the single BiLSTM approach. This testifies that the hybrid fusion indeed captures both feature-level and temporal relationships. In the computation cost, the RF-BiLSTM model provides in average a training time of 12.8 minutes and an inference latency of 4.3 ms per sample in Kaggle T4 GPU environment, compared with RF: 8.6 minutes / 2.9 ms and BiLSTM: 11.4 minutes / 6.8 ms. This indicates that the repeated model is still computationally viable and provides significantly improved detection reliabilities.

6.7. Scalability and Deployment Feasibility

The proposed RF–BiLSTM framework exhibits strong potential for scalability in edge- and fog-level environments. Because the Random Forest component performs early feature reduction. The dimensionality of input sequences to BiLSTM is substantially reduced, minimizing memory and communication overheads. The lightweight two-layer BiLSTM architecture was intentionally chosen to maintain low computational demand, indicating that the model could be efficiently executed on mid-range IoT edge devices such as NVIDIA Jetson Nano (4 GB RAM) or Raspberry Pi 5 with GPU support. Furthermore, the modular design allows near-real-time inference through batch-window processing without retraining. This is suggesting adaptability for continuous monitoring in domains like smart homes, healthcare, and industrial IoT networks.

6.8. Limitations and Future Work

While the RF-BiLSTM model demonstrates high accuracy (99.87 %) and low FAR (0.13 %), its performance was validated on a single benchmark dataset (Aposemat IoT-23). Future work will focus on testing across heterogeneous IoT datasets to enhance generalization and robustness. Additionally, we plan to extend the framework toward zero-day attack detection and online incremental learning, enabling adaptive responses to emerging threat patterns in dynamic IoT networks. Energy-efficient training and model compression strategies will also be investigated to improve deployability on resource-limited devices.

7. Conclusion

This research successfully designed and developed a novel yet robust attack detection model for IoT networks. This research analyzed existing ML models developed for securing IoT data in previous literary works available. Considering the advantages of the hybrid ML algorithms and limitations of other conventional ML algorithms, this work give a RF-BiLSTM model along with a MOGA based feature extraction approach. The proposed RF-BiLSTM based attack detection model will be trained to identify and classify the unusual behaviour from the network traffic with high accuracy and minimum false detection rate. The implementation of the metaheuristic MOGA algorithm is improved the computation time with a lesser number of resources. The proposed hybrid RF-BiLSTM model, combined with a MOGA-based feature extraction approach, demonstrated superior performance in detecting and classifying unusual behaviour in network traffic. By integrating Random Forest (RF) for efficient feature selection and probabilistic prediction refinement with Bidirectional Long Short-Term Memory (BiLSTM) networks for sequential learning, the model achieved exceptional accuracy of 99.87% while minimizing false positives and negatives. This model also achieved an excellent trade off between the performance and cost effectiveness and thereby demonstrates how the proposed approach can be used to detect real-time cyber-attacks in IoT. This research work also proved the feasibility and effectiveness of hybrid machine learning algorithms in improving IoT cyber security and open a new ways for significantly contributes in future research in the area of anomaly detection and real-time IoT threat analysis.While the model achieved strong results, future work will focus on extending it toward zero-day attack detection and lightweight adaptive learning to improve scalability on resource-constrained IoT devices. Addressing these aspects will make the proposed RF–BiLSTM framework an even more reliable and versatile solution for securing next-generation IoT ecosystems.

Acknowledgements.

The authors gratefully acknowledge the infrastructure and computational support provided under the DST-FIST (Fund for Improvement of S&T Infrastructure) programme at Jamia Hamdard, New Delhi, which greatly facilitated the successful completion of this research.

References

[1] Atlam HF, Wills GB. IoT security, privacy, safety and ethics. In: *Digital Twin Technologies and Smart Cities 2020*; 2020. p. 123–149.

[2] Alladi T, Chamola V, Sikdar B, Choo KKR. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* 2020; 9(2):17–25.

[3] Lu Y, Da Xu L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things J.* 2019; 6(2):2103–2115.

[4] Khader R, Eleyan D. Survey of DoS/DDoS attacks in IoT. *Sustainable Engineering and Innovation.* 2021; 3(1):23–28.

[5] Sharmeen S, Huda S, Abawajy JH, Ismail WN, Hassan MM. Malware threats and detection for industrial mobile-IoT networks. *IEEE Access.* 2018; 6:15941–15957.

[6] Sharma V, Kim J, Kwon S, You I, Lee K, Yim K. A framework for mitigating zero-day attacks in IoT. *arXiv preprint* arXiv:1804.05549; 2018.

[7] Ali I, Ahmed AIA, Almogren A, Raza MA, Shah SA, Khan A, Gani A. Systematic literature review on IoT-based botnet attack. *IEEE Access.* 2020; 8:212220–212232.

[8] Litoussi M, Kannouf N, El Makkaoui K, Ezzati A, Fartitchou M. IoT security: Challenges and countermeasures. *Procedia Comput. Sci.* 2020; 177:503–508.

[9] Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, et al. Deep learning and big data technologies for IoT security. *Comput. Commun.* 2020; 151:495–517.

[10] Boukerche A, Coutinho RW. Design guidelines for machine learning-based cybersecurity in Internet of Things. *IEEE Netw.* 2021; 35(1):393–399.

[11] Strecker S, Van Haaften W, Dave R. An analysis of IoT cybersecurity driven by machine learning. In: *Proc. Int. Conf. Communication and Computational Technologies*; 2021. p. 725–753.

[12] Alrashdi I, Alqazzaz A, Aloufi E, Alharthi R, Zohdy M, Ming H. AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning. In: *2019 IEEE Computing and Communication Workshop and Conference (CCWC)*; 2019. p. 0305–0310.

[13] Kotenko I, Izrailov K, Buinevich M. Static analysis of information systems for IoT cybersecurity: A survey of machine learning approaches. *Sensors.* 2022; 22(4):1335.

[14] Tyagi H, Kumar R. Attack and anomaly detection in IoT networks using supervised machine learning approaches. *Rev. Intell. Artif.* 2021; 35(1):11–21.

[15] Dalal KR. Analysing the role of supervised and unsupervised machine learning in IoT. In: *2020 Int. Conf. Electronics and Sustainable Communication Systems (ICESC)*; 2020. p. 75–79.

[16] Rezaei A. Using ensemble learning technique for detecting botnet on IoT. *SN Comput. Sci.* 2021; 2(3):1–14.

[17] Aurangzeb S, Anwar H, Naeem MA, Aleem M. BigRC-EML: Big-data based ransomware classification using ensemble machine learning. *Cluster Comput.* 2022; 1–18.

[18] Hsu HT, Jong GJ, Chen JH, Jhe CG. Improve IoT security system of smart-home using SVM. In: *2019 IEEE Int. Conf. Computer and Communication Systems (ICCCS)*; 2019. p. 674–677.

[19] Guo C, Zhuang R, Su C, Liu CZ, Choo KKR. Secure and efficient k-NN query over encrypted uncertain data in cloud-IoT ecosystem. *IEEE Internet Things J.* 2019; 6(6):9868–9879.

[20] Hanif S, Ilyas T, Zeeshan M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In: *2019 IEEE Int. Conf. Smart Cities (HONET-ICT)*; 2019. p. 152–156.

[21] Ahmad Z, Shahid Khan A, Nisar K, Haider I, Hassan R, Haque MR, Rodrigues JJ. Anomaly detection using deep neural network for IoT architecture. *Appl. Sci.* 2021; 11(15):7050.

[22] Kaur P, Kumar R, Kumar M. A healthcare monitoring system using random forest and IoT. *Multimed. Tools Appl.* 2019; 78(14):19905–19916.

[23] Fatayer TS, Azara MN. IoT secure communication using ANN classification algorithms. In: *2019 Int. Conf. Promising Electronic Technologies (ICPET)*; 2019. p. 142–146.
[24] Saharkhizan M, Azmoodeh A, Dehghantanha A, Choo KKR, Parizi RM. An ensemble of deep RNNs for detecting IoT cyber attacks using network traffic. *IEEE Internet Things J.* 2020; 7(9):8852–8859.
[25] Hikal NA, Elgayar MM. Enhancing IoT botnet attack detection using ML-IDS and ensemble preprocessing. In: *Internet of Things—Applications and Future*; 2020. p. 89–102.
[26] Tomer V, Sharma S. Detecting IoT attacks using an ensemble machine learning model. *Future Internet.* 2022; 14(4):102.
[27] Jayalaxmi PLS, Saha R, Kumar G, Kim TH. Machine and deep learning amalgamation for feature extraction in IIoT. *Comput. Electr. Eng.* 2022; 97:107610.
[28] Thakkar A, Lohiya R. A review on ML and DL perspectives for IDS in IoT. *Arch. Comput. Methods Eng.* 2021; 28(4):3211–3243.
[29] Hazer-Rau D, Arends R, Zhang L, Traue HC. Feature selection using evolutionary algorithms for affective computing. *Eng. Proc.* 2021; 10(1):42.
[30] Strecker S, Dave R, Siddiqui N, Seliya N. A modern analysis of aging ML-based IoT cybersecurity methods. *arXiv preprint* arXiv:2110.07832; 2021.
[31] Usoh M, Asuquo P, Ozuomba S, et al. A hybrid ML model for detecting cybersecurity threats in IoT applications. *Int. J. Inf. Technol.* 2023; 15:3359–3370.
[32] Sajid M, Malik KR, Almogren A, et al. Enhancing intrusion detection: A hybrid machine and deep learning approach. *J. Cloud Comput.* 2024; 13:123.
[33] Yaras S, Dener M. IoT-based intrusion detection using a new hybrid deep learning algorithm. *Electronics.* 2024; 13(6):1053.
[34] Behiry MH, Aly M. Cyberattack detection in WSN using hybrid feature reduction with AI and ML. *J. Big Data.* 2024; 11:16.
[35] García S, Parmisano A, Gómez MI. IoT-23: A labeled dataset for malicious and benign IoT network traffic. Stratosphere Laboratory, CTU Prague; 2020.
[36] Akuthota UC, Bhargava L. Transformer-based intrusion detection for IoT networks. *IEEE Internet Things J.* 2025; 12(5):6062–6067.
[37] Vyas A, Lin PC, Hwang RH, Tripathi M. Privacy-preserving federated learning for intrusion detection in IoT. *IEEE Access.* 2024; 12:127018–127050.