Deep Learning based DDoS Attack Detection in Internet of Things: An Optimized CNN-BiLSTM Architecture with Transfer Learning and Regularization Techniques

Iqbal Jebril [1], M. Premkumar [2], Ghaida Muttashar Abdulsahib [3], S. R. Ashokkumar [4], S. Dhanasekaran [5],
Oshamah Ibrahim Khalaf [6], and Sameer Algburi [7]

***Abstract*—In recent days, with the rapid advancement of technology in informatics systems, the Internet of Things (IoT) becomes crucial in many aspects of daily life. IoT applications have gained popularity due to the availability of various IoT enabler gadgets, such as smartwatches, smartphones, and so on. However, the vulnerability of IoT devices has led to security challenges, including Distributed Denial-of-Service (DDoS) attacks. These limitations result from the dynamic communication between IoT devices due to their limited data storage and processing resources. The primary research challenge is to create a model that can recognize legitimate traffic while effectively protecting the network against various classes of DDoS attacks. This article proposes a CNN-BiLSTM DDoS detection model by combining three deep-learning algorithms. The models are evaluated using the CICIDS2017 dataset against commonly used performance criteria which the models perform well, achieving an accuracy of around 99.76%, except for the CNN model, which achieves an accuracy of 98.82%. The proposed model performs best, achieving an accuracy of 99.9%.**

***Index Terms*—Classification, CNN+BiLSTM, DDOS attacks, deep learning, IoT.**

I. Introduction

The DDoS attacks are a major threat to wireless sensor networks (WSNs), which are networks of small and low-power devices that collect and transmit data from their surrounding environment. In a WSN, DDoS attacks can be launched to overwhelm the network's resources and disrupt its normal operations, leading to service degradation or complete failure. The WSNs are vulnerable to DDoS attacks due to their limited resources and their distributed nature, which makes it difficult to mitigate attacks. In addition, WSNs may be deployed in harsh and unsecured environments, making them more susceptible to attacks.

The IoT devices are interconnected objects that collect and communicate data over internet, and it often deployed in critical infrastructure such as healthcare, transportation, and industrial control systems.

DDoS attacks in WSNs can take various forms, such as flooding attacks, resource depletion attacks, and sinkhole attacks. Flooding attacks involve creating the traffic, while resource depletion attacks target the network's resources, such as memory or battery, by sending malicious data packets. Sinkhole attacks involve redirecting network traffic to a malicious node, which can intercept or modify the data.

To protect WSNs against DDoS attacks, various defense mechanisms have been proposed, such as intrusion detection systems, data aggregation, and collaborative filtering. These mechanisms aim to detect and mitigate attacks by analyzing network traffic, detecting anomalies, and filtering out malicious packets. The DDoS attacks in WSNs pose a significant threat to security and reliability. This require effective defense mechanisms to ensure their proper functioning.

DDoS attacks in IoT can be launched to overwhelm the devices or network infrastructure with a large volume of traffic, leading to service degradation or complete failure. It can take various forms, such as botnet attacks, amplification attacks, and protocol attacks. Botnet attacks involve compromising a huge figure of IoT devices and using them to launch coordinated DDoS attacks. Protocol attacks involve targeting the vulnerabilities in the communication protocols used by IoT devices, such as the MQTT protocol.

To defend IoT devices against DDoS attacks, various defense techniques have been proposed, such as anomaly detection, traffic filtering, and cloud-based defenses. These mechanisms aim to detect and mitigate attacks by analyzing network traffic, filtering out malicious traffic, and diverting traffic to cloud-based services for further analysis. Overall, to improve the reliability devices and networks, and require effective defense mechanisms to ensure their proper functioning.

[1] Department of Mathematics, Al-Zaytoonah University of Jordan, Amman, Jordan (e-mail: i.jebril@zuj.edu.jo)

[2] Department of Electronics and Communication Engineering, SSM Institute of Engineering and Technology, Dindigul, Tamil Nadu, India (e-mail: prem53kumar@gmail.com)

[3] Department of Computer Engineering, University of Technology, Baghad, Iraq (e-mail: ghaida.m.abdulsaheb@uotechnology.edu.iq)

[4] Centre for Block-Chain and Cybersecurity, Department of Computer and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India (e-mail: srashokkumar1987@gmail.com)

[5] Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India (e-mail: dhanselvaraj@gmail.com)

[6] Department of Solar, Al-Nahrain Research Center for Renewable Energy, Al-Nahrain University, Jadriya, Baghdad, Iraq (e-mail: usama81818@nahrainuniv.edu.iq)

[7] Al-Kitab University, College of Engineering Technology, Kirkuk, Iraq (e-mail: sameer.algburi@uoalkitab.edu.iq)

DOI: 10.36244/ICJ.2024.1.1

The authors in [1] proposed IDS for WSNs that uses a rule-based approach to defend the DDoS attacks. The system monitors the traffic at each node and sends alerts to the base station when an attack is detected.

Data aggregation involves collecting and processing data at the nodes near to BS which reduces the amount of traffic. This can help to prevent flooding attacks and reduce the impact of DDoS attacks. The authors in [2] proposed a data aggregation scheme for WSNs that uses a fuzzy logic- to identify and filter out malicious traffic.

Collaborative filtering involves nodes in the network exchanging information to discover the malevolent traffic. Nodes can share information about the types of packets received and the sources of the traffic to defend the attacks. The authors in [3] proposed a collaborative filtering scheme for WSNs that uses a reputation-based approach to defend malevolent traffic.

The ML techniques can be used to train the system to classify patterns in network traffic and detect the DDoS attacks [4]. Dynamic thresholding involves setting thresholds for network traffic based on the network conditions and adjusting them dynamically to accommodate changes in the traffic. The authors in [5] proposed a dynamic thresholding approach in WSNs using the moving average and standard deviation of the network traffic.

II. RELATED WORKS

To defend IoT devices against DDoS attacks, various defense techniques have been proposed. The paper [6] proposes various kind of DDoS attacks and the techniques used to launch them. It also provides an extensive review of different mechanisms used to diminish DDoS attacks. The paper classifies DDoS attacks into various categories, in which the authors discuss the attack characteristics, how they work, and the methods used to mitigate them. It also presents a survey of various tools and technologies used for DDoS attack detection and mitigation.

The several defense mechanisms used to counter the DDoS attacks which include filtering techniques such as packet filtering, source address filtering, and rate limiting. They also discuss other approaches such as anomaly detection, traceback, and redirection. It highlights the limitations of existing defense mechanisms and suggesting areas for future research [6].

Table 1 serves as a comprehensive comparison of literature, key parameters such as accuracy, precision, recall, and F1-score, alongside other essential evaluation metrics for each dataset and corresponding model.

The ML based DDoS detection and mitigation system for SDNs is proposed to categorize the normal or malicious traffic. The system is designed to work in SDNs, which allow for centralized network control and management [7]. From the performance of various ML algorithms, RF algorithm performs the best, with an accuracy of 98.2% and low FPR in SDN environment. It is compared with other IDS in which they find that it outperforms in terms of accuracy, detection rate, and FPR. They suggest that their system can be further improved by incorporating other features, such as flow-based features and temporal features. The paper demonstrates the possible of ML algorithms for DDoS mitigation in SDNs.

Paper [8] proposes an anomaly-based approach to identify DDoS attacks using SVM classifiers. The performance of the SVM classifier is compared with DT and KNN in CAIDA using different evaluation metrics. They find that their SVM classifier can effectively detect attacks with a maximum DR and a minimum FPR. The authors also analyze the SVM classifier under different flooding attack scenarios in which it can detect these attacks with high accuracy and low FPR. This approach can be improved by incorporating additional parameters like packet entropy.

The paper [9] proposes a semi-supervised approach for network traffic classification and fine-grained flow identification using hierarchical deep neural networks. The dataset of network traffic is used to train and test DNN models. Dataset includes both labeled and unlabeled traffic data. The FlowPrint technique is to extract fine-grained flow features from network traffic data. FlowPrint is a representation learning technique that captures the underlying structure of network traffic flows. A hierarchical deep neural network architecture that uses the FlowPrint features for network traffic classification. The hierarchical architecture allows for interpretability and explainability of the classification results.

The performance of the approach is evaluated using different evaluation. The proposed [9] results shows that the approach can accurately classify network traffic with high precision and recall. The authors Zhang et. al [9] conclude that their semi-supervised approach using hierarchical deep neural networks and FlowPrint features is an effective technique for network traffic classification and fine-grained flow identification.

The paper [10] highlights the importance of using big data analytics for DDoS detection, as DDoS attacks generate a large amount of traffic data that needs to be analyzed in real-time. This paper provides an overview about techniques and tools used for big data analytics in DDoS detection, including ML, DL, clustering, and rule-based approaches. It discusses the pros and cons of each technique and tool, and provides examples of recent studies that have used these techniques for DDoS detection. The paper also discusses the challenges and issues involved in DDoS detection, such as the high cost of data storage and processing, and the lack of standardization and interoperability among different tools and techniques. But more efficient and scalable big data analytics techniques for DDoS detection are needed, as well as on improving the accuracy and reliability of these techniques.

The paper [11] provides the details of work carried recently in the field of DDoS attack mitigation techniques. The paper provides an outline of DDoS attacks, characteristics of each type of attack, the vulnerabilities they exploit, and their impacts on the target system. It reviews the different DDoS attack mitigation techniques, including network, host and hybrid level defenses. The challenges and issues of each mitigation method, and provides examples of recent studies are discussed that have used for detection techniques. It also discusses the challenges and issues involved in DDoS attack mitigation, the difficulty of distinguishing between normal and illegitimate activity, and cost of implementing mitigation techniques. The more efficient and effective DDoS attack mitigation techniques, as well as on improving the collaboration and coordination among different stakeholders in the mitigation process.

The paper [21] provides recent research in the field of DDoS attack mitigation techniques. It highlights the different kind of attacks and the vulnerabilities they exploit, and provide an overview of the different defense techniques that can be used to protect against these attacks. The paper also identifies the challenges and issues involved in DDoS attack mitigation and suggest future research directions to address these challenges.

Analyzing the information presented in Table 1, the research demonstrates that the utilization of machine learning-based methods proves successful in identifying attacks. This effectiveness is notably enhanced when these approaches are combined with supplementary techniques such as feature selection and preprocessing. Moreover, the detection of DDoS attacks in wireless sensor networks introduces unique and specific challenges

TABLE I
Comparison of Literature

Dataset/Model	**Author Details**	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Other Evaluation Metrics**
NSL-KDD	Mohammed et al [7]	0.999	-	-	-	FPR 0.01%, FNR 0%
NSL-KDD	Garcia et al [12]	0.991	0.972	0.992	0.982	DR 99.2%, FAR 0.8%
CICIDS2017/CNN	Hayyolalam et al [11]	0.99	0.997	0.995	0.996	-
CICIDS2017/SAE	Catak et al [13]	0.99	0.9978	0.999	0.9983	-
CICIDS2017/CNN+LSTM	Nguyen et al [14]	0.985	0.96	0.99	0.97	-
DARPA/MLP	Yin et al [15]	0.996	0.997	0.996	0.996	-
DARPA/DBN	Li et al [16]	0.987	0.991	0.982	0.986	-
DARPA/RF	Farukee et al [17]	0.9795	0.981	0.977	0.979	FPR 1.25%, FNR 2.3%
KDD99/CNN	Ye et al [18]	0.9984	0.998	0.998	0.9982	DR 99.86%, FPR 0.01%
KDD99/GRU	Alghazzawi et al [19]	0.999	-	-	-	FPR 0.07%, FNR 0.02%
NSL-KDD/RNN	Aswad et al [20]	0.9828	0.9738	0.981	0.9762	FPR 2.62%, FNR1.88%
NSL-KDD/CNN	Saini et al [21]	0.9933	0.9929	0.993	0.9927	DR 99.37%, FPR 0.02%
CICIDS2017/CNN	Shang et al [22]	0.9991	-	-	-	FPR 0.03%, FNR 0.05%
UNSW-NB15/LSTM	Yousuf et al [23]	0.9967	0.9968	0.997	0.9967	FPR 0.1%, FNR 0.23%
UNSW-NB15/CNN	Alshehadeh et al [24]	0.9936	0.9944	0.994	0.994	DR 99.4%, FPR 0.04%

III. SYSTEM MODEL

A system model for DDoS attack detection using deep learning is shown in figure 1. It typically involves the first step as building a system is to collect data from the network. This data can include network traffic data, packet header data, and flow data. After data collection, it needs to be preprocessed to prepare it for analysis. The initial stage of the process involves extracting relevant features, normalizing the data, and filtering out unnecessary information. In the following phase, the preprocessed data is used to train DL model. The weights are adjusted to reduce the difference between expected and actual outputs. Once training is complete, a separate dataset is employed to evaluate the model and identify potential issues. Subsequently, the model can be utilized for real-time detection of DDoS attacks in a production setting, following successful training and testing.

At outset of the workflow, the input is obtained, either in its raw form or after preprocessing. Feature extraction is carried out, whereby significant characteristics are identified from the input data, including packet size, packet count, and protocol type. These extracted features are then entered into a deep neural network that may comprise a CNN, RNN, or a hybrid of both. The deep neural network processes the input data and assimilates the patterns and correlations between features that signify DDoS attacks.

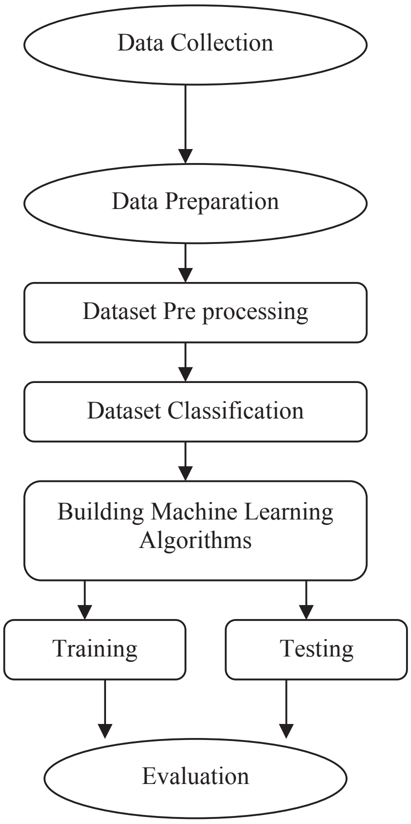

Fig. 1. System model

Finally, the output of DNN is analyzed to decide the data as normal network traffic or a DDoS attack. If a DDoS attack is detected, appropriate mitigation strategies can be employed to prevent it from causing harm to the network.

A. CNN Algorithm

Let X be the input traffic data with shape (batch $_{size,}$ sequence $_{length}$, input $_{dim}$), where batch $_{size}$ denotes samples count, sequence $_{length}$ is the time sequence length, and input $_{dim}$ denotes number of features in each time step.

The CNN-based deep learning algorithm can be represented as follows:

- Input layer: X with shape (batch $_{size,}$ sequence $_{length}$, input $_{dim}$)
- Convolutional layer: apply a set of filters with size (filter $_{size,}$ input $_{dim}$) to the input data X, resulting in a set of feature maps.
- Max pooling layer: extract each feature map value to diminish the dimensionality of the feature maps.
- Flatten layer: 2D maps are renewed into a 1D vector.
- Fully connected layer: apply a set of weights to the flattened vector to acquire a hidden value of the input data.
- Output layer: softmax is applied to the hidden representation to obtain predicted class probabilities.

Let W_1, W_2... W_k be the set of convolutional filters, where k is the number of filters. Each filter Wj can be represented as a 2D matrix with size (filter $_{size,}$ input $_{dim}$). The output feature map corresponding to filter Wj can be represented as follows

$$Fj=max(0,Wj*X+b\ j) \qquad (1)$$

where * denotes the convolution operation, bj is the bias term, and max(0, x) is ReLU function. Let V be the weight matrix with shape (num $_{classes,}$ hidden $_{size}$). The output can be represented as follows:

$$H=relu(W*F+b) \qquad (2)$$

where W = V^T, b is the bias term, and relu(x) = max(0, x) is ReLU function.

The final predicted class probabilities can be calculated by applying the softmax to the output of the fully connected layer:

$$P=soft\ max(H) \qquad (3)$$

where P is a vector of length, representing the predicted class probabilities. The model parameters can be learned by minimizing a suitable loss function using SGD. One approach to train a model for detecting DDoS attacks is to use a labeled dataset of traffic data. In this dataset, each sample is marked as either normal or DDoS traffic.

B. Dataset

The CICIDS2017 [26] is a dataset of network traffic designed for intrusion detection research. It was created by the Canadian Institute for Cybersecurity at the University of New Brunswick in Canada. The dataset includes benign and malicious traffic captured in a real network environment. The malicious traffic includes various kind of attacks such as DoS, DDoS, brute-force attacks, and more. The dataset also includes a variety of network protocols such as HTTP, FTP, TCP, UDP, ICMP, etc.

TABLE II
CICIDS 2017 DATASET DESCRIPTION

Attack Type	Number of Instances	Average Packet Size	Average Flow Duration	Average Fwd Segments	Average Bwd Segments	Max Fwd Packet Length	Max Bwd Packet Length	Fwd Packet Length Std	Bwd Packet Length Std
DoS Hulk	231073	1392.5	46353.5	7.28	3.09	1472	1460	187.6	371.5
DoS GoldenEye	102157	1503.8	36753.1	13.54	3.04	1472	1460	212.1	365.9
DoS slowloris	11586	746.16	40393.5	2.17	2.62	590	589	136.2	142.7
DoS Slowhttptest	549	3104.4	1156624	10.49	7.52	1480	1476	89.15	172.3
Heartbleed	1000	707.6	60483.9	9.62	10.3	177	202	159.7	44.52
Infiltration	36	1352.4	45564.0	22.39	11.3	1472	1472	0.00	0.00
Bot	196907	1468.8	12686.0	10.22	4.90	1472	1472	39.51	237.8
PortScan	158930	882.1	405.44	6.47	4.52	1472	1408	300.6	451.4
Web Attack - XSS	652	1718.2	15838.0	8.28	6.18	1472	1472	206.6	309.0

C. CNN+BiLSTM based deep learning algorithm

CNN+BiLSTM is a DL architecture that combines CNN and BiLSTM in which the CNN is responsible for feature extraction from input data. It consists of multiple filters that slide over the input data and extract local features. Then the output is fed to the BiLSTM layer which is a type of RNN that has the ability to form sequential data. This layer takes the output of the CNN layer and processes it in both forward and backward directions. This allows capturing both past and future contexts of the data. The output of the BiLSTM layer to a fixed number of classes, which in the case of DDoS attack detection corresponds to normal traffic and DDoS traffic. The output is then passed through a softmax function to calculate the final prediction probabilities for each class. The CNN+BiLSTM architecture can be trained using backpropagation and weights are updated iteratively during the training to optimize the model performance in shown in Fig 2.

Let x be a wireless sensor network traffic sequence with m features and n time steps. Let y be the corresponding binary label sequence, where 0 represents non-attack traffic and 1 represents DDoS attack traffic. The mathematical model for identifying DDoS attacks in WSN using CNN+BiLSTM based deep learning algorithm can be represented using the following equations.

Apply a 1D CNN layer with k filters of size f on the input x to extract k feature maps of n-f+1 size. Use ReLU activation function and apply max pooling operation on each feature map to reduce the dimensionality by a factor of p. Let the input features be represented by X ∈ R^(n x m), where n is samples count and m is feature count.

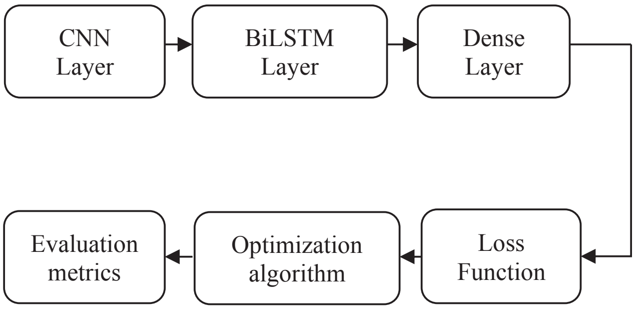

Fig 2. Proposed method workflow

The CNN can be represented using the following equations

$$Yi=\max_{pool}(W*Xi+b) \qquad (4)$$

Here, Yi denotes the output feature map of the ith filter, W represents the weight of the ith filter, Xi is the input feature map, b stands for the bias term, and $\max_{pool}$ signifies the max-pooling operation.

The BiLSTM can be represented using the following equations-

$$f_t = \sigma(W_f *[h_{t-1}, x_t]+b_f \qquad (5)$$

$$i_t = \sigma(W_i *[ht -1\}, x_t]+b_i \qquad (6)$$

$$o_t = \sigma(W_o *[ht -1\}, x_t]+b_o \qquad (7)$$

$$g_t = \tanh(W_c *[ht -1\}, x_t]+b_c \qquad (8)$$

$$c_t = f_t * c_{t-1} + i_t * g_t \qquad (9)$$

$$h_t = o_t * \tanh(c_t) \qquad (10)$$

Apply a fully connected dense layer on the BiLSTM layer with o output units and sigmoid to generate o binary predictions.
Let the output layer be represented by Ŷ ∈ R^n, where n is the number of samples. The output of the network can be represented using the following equation

$$\hat{Y}=\text{softmax}(W_Y*hn+b_y) \qquad (11)$$

where hn is the output of BiLSTM, W_Y is output layer weight, and b_y is the bias term. The DDoS detection can be done by comparing Ŷ with Y. If Ŷ is significantly different from the actual output Y, then it can be classified as a DDoS attack.

The mathematical model can be trained using backpropagation with cross-entropy loss as the objective function. The training process involves minimizing the objective function with respect to the model parameters. This can be done using gradient descent or any of its variants.

D. Algorithm

1 Load and preprocess the dataset.

2 Convert the text to numerical vectors using word embeddings. Let the input is X = (x1, x2, ..., xn), where each xi is a d-dimensional word embedding vector.

3 Split the data into training and testing sets.

4 Identify the CNN layer with filters of varying sizes. Let the filters have sizes f1, f2, ..., fk, where each fk is a vector of length h. Let the filters count be denoted by m. For each filter fk, convolve it with X to acquire feature maps: fk_i = relu((Wfk * X[i:i+h-1] + bfk)) where Wfk is the weight matrix and bfk is the bias vector associated with filter fk, and relu is the ReLU function.

5 Apply max pooling on the feature maps to get a fixed-length output. For each feature map fk_i, apply max pooling to obtain the maximum value: gk = max(fk_1, fk_2, ..., fk_n-h+1)

6 Concatenate the output from the max pooling layer with BiLSTM layer. Let the concatenated output is Z where each zi is a scalar value obtained by concatenating gk with BiLSTM layer.

7 Define the BiLSTM layer with a certain number of hidden units. Let the hidden size of the BiLSTM layer be denoted by p. Apply a BiLSTM layer to the input sequence X to obtain the output sequence Y.

8 Concatenate the output from the BiLSTM layer with the output from the max pooling layer. Let the concatenated output be denoted by Z.

9 Add a fully connected layer with a softmax activation function for classification. Let the number of classes be denoted by C. Apply a Z to obtain the output vector o, where o = softmax(Wo * Z + bo), and Wo is the weight matrix and bo is the bias vector associated with the fully connected layer.

10 Train the model on the training set using cross-entropy loss. Let the training set be denoted by D and each yi is a one-hot encoded label vector.

11 Calculate the model on the testing set using accuracy or other evaluation metrics.

12 Repeat steps 4-11 with different hyperparameters (e.g., number of filters, filter sizes, number of hidden units) to find the best model.

Some simulation parameters that shown in Table 3 could be used for DDoS detection using a CNN+BiLSTM algorithm.
The first step in setting up a simulation experiment is to choose a dataset. In order to train the CNN+BiLSTM model, a set of input features must be selected. These features could include information such as the IP addresses, the protocol used, and time stamp of each network packet. The hyperparameters of the CNN+BiLSTM model must be defined. These include the number and size of filters in CNN layer, the hidden units in BiLSTM layer, and learning rate used during training. In order to train, a choice of parameters need to be specified, and optimizer to be utilized. Once the model is trained, its performance can be assessed using a separate testing set, with evaluation metrics for classifying a network flow as normal or an attack being among the testing parameters. The Longer simulation duration may be required to achieve higher accuracy levels. Finally, the specifications used to run the simulation should be taken into account. The specifications can include the CPU and GPU, the memory, and the disk space required to store the dataset and model.

IV. Results and Discussions

TABLE III
SIMULATION PARAMETERS

Parameter	Value
Dataset	DARPA 1998
Pre processing	One-hot encoding, normalization
Training-Validation split	70-30
Model Architecture	CNN+BiLSTM
Number of layers	CNN:2; BiLSTM:128
Number of filters	CNN:64, 128; BiLSTM:128
Filter Size	CNN: 3x3, 5x5; BiLSTM: N/A
Dropout rate	0.5
Learning rate	0.001
Batch Size	128
Number of epochs	50
Loss function	Binary cross-entropy
Evaluation metric	Accuracy, precision, recall, F1-score
Hardware	NVIDIA GeForce GTX1080 Ti
Software	Python 3.7, Tensor Flow 2.3.1

The simulation parameters will help in conducting experiments to test the performance of the proposed model for DDoS detection. The aim should be to optimize the hyperparameters and training parameters to achieve the results.
The parameters mentioned above can be customized according to the unique attributes and needs of both the dataset and the model. The confusion matrix presents the counts of TP, FP, FN and TN. Meanwhile, the ROC curve AUC score is utilized to gauge probability thresholds.

Accuracy: The proportion of correctly classified samples out of the total number of samples.

$$\text{Accuracy} = \frac{(\text{TP}+\text{TN})}{(\text{TP}+\text{TN}+\text{FP}+\text{FN})} \qquad (12)$$

Precision: It measures the ability of the model to correctly identify positive samples.

$$\text{Precision} = \frac{\text{TP}}{(\text{TP}+\text{FP})} \qquad (13)$$

Recall: It measures the ability of the model to identify all positive samples.

$$\text{Recall} = \frac{\text{TP}}{(\text{TP}+\text{FN})} \qquad (14)$$

F1-score: It provides a balance between precision and recall.

$$\text{F1-score} = \frac{2 * \text{Precision} * \text{Recall}}{(\text{Precision} + \text{Recall})} \qquad (15)$$

TABLE IV
PERFORMANCE COMPARISON OF THE PROPOSED METHOD

Model	Accuracy	Error	Precision	Recall	f-1score
RNN [15]	0.996	0.018	0.987	0.983	0.985
BiLSTM [19]	0.998	0.014	0.989	0.992	0.991
LSTM [12]	0.997	0.011	0.911	0.935	0.91
CNN [20]	0.988	0.036	0.977	0.983	0.98
KNN [25]	0.967	0.013	0.976	0.982	0.982
Proposed	0.999	0.012	0.998	0.999	0.997

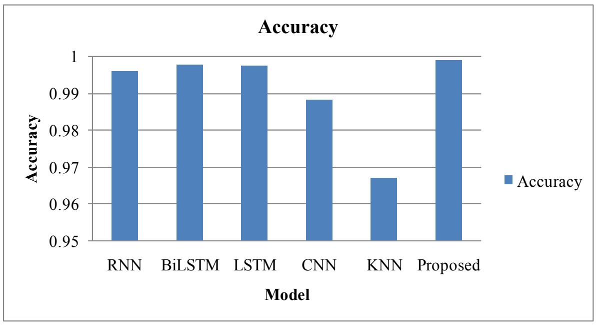

Fig 3. Model Vs Accuracy

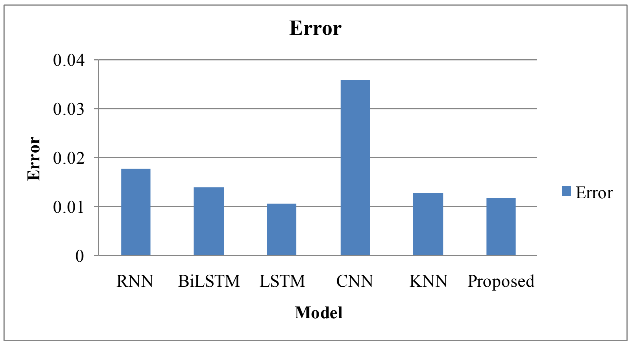

Fig 4. Model Vs Error

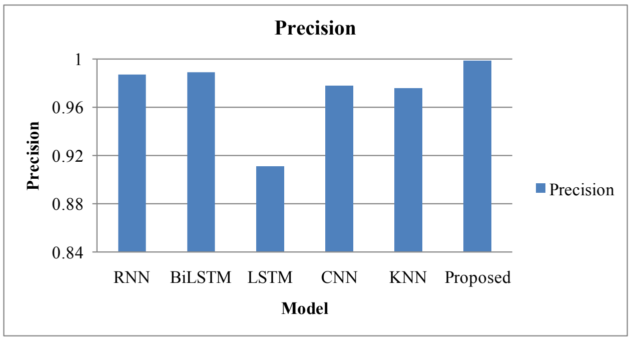

Fig 5. Model Vs Precision

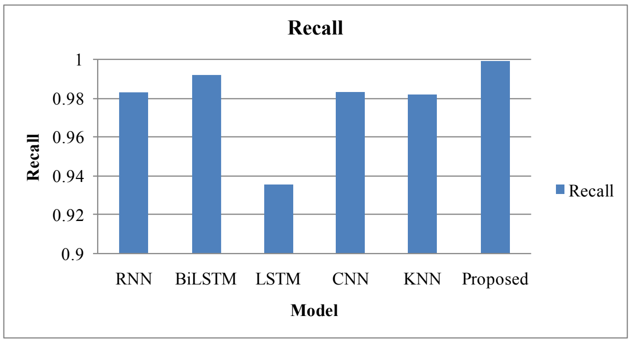

Fig 6. Model Vs Recall

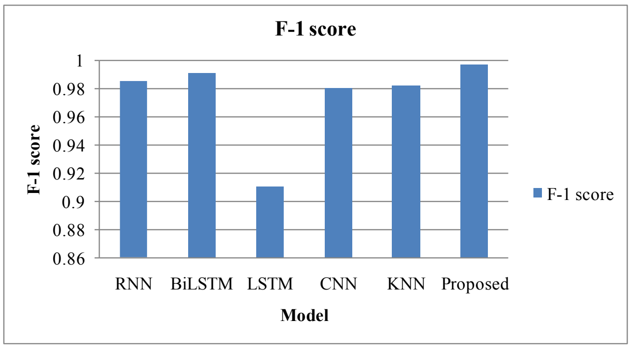

Fig 7. Model Vs F-1 score

Performance of the detection system is evaluated by performance metrics. Figures 3-7 show the plot of detection parameters for various classification models. In figure 3, the

RNN and Proposed models exhibited superior accuracy at 99.9%, closely followed by the BiLSTM model at 99.8%, while the LSTM and CNN models achieved slightly lower accuracies at 99.7% and 98.8% respectively. Concerning the error rate in figure 4, the Proposed, RNN, and BiLSTM models maintained impressively low values at 1.1-1.8%, signifying their robustness in the classification task. In terms of precision the figure 5 shows, the BiLSTM and Proposed models performed exceptionally well at 99%, closely followed by the RNN and CNN models, which achieved high precision values of 98%. In figure 6, the recall values were consistent across most models, with the Proposed, RNN, BiLSTM, and CNN models showcasing strong recall rates at 98-99%. Similarly, the figure 6 shows the F1-score reflected the models' overall performance, with the BiLSTM, Proposed, and RNN models demonstrating the highest scores at 98-99%, followed closely by the CNN and KNN models, which achieved competitive F1-scores at 98%. According to the result in Table 4, the accuracy of the proposed method is 99.9 % which can be improved by increasing the training samples. Error is 1.16%, precision is 99.8%, recall is 99.9% an F-1 score
is 99.7%.

TABLE V
CONFUSION MATRIX FOR THE PROPOSED METHOD

Actual/ Predicted	Class 1	Class 2	Class 3	Class 4	Class 5	Class 6
Class 1	- 180000	9	12	420	55	6
Class 2	30	42000	0	2	0	0
Class 3	3	0	3300	21	2	1
Class 4	80	0	0	76000	0	0
Class 5	16	0	1	1	1800	13
Class 6	9	0	0	0	18	2000

Table 5 displays a confusion matrix, which serves as an assessment tool for a classification model's effectiveness. It operates by contrasting the forecasted labels with the genuine labels of a test dataset. The composition of the confusion matrix for the CNN+BiLSTM approach will be influenced by the specific task at hand and the quantity of classifications present in the data collection.

V. CONCLUSIONS

DDoS attacks are a significant threat and they are difficult to detect because attackers use spoofing technology. Traditional detection systems have been ineffective against historically potent botnets like Mirai and Bashlite. IoT networks, in particular, are at risk of cyberattacks and require strong protective measures. The proposed model achieves an average accuracy of 99.76% in identifying DDoS attacks, surpassing the performance of other tested models. However, the authors caution against overlooking the accuracy of the other three classifiers, which achieve an average accuracy of 99.16%. The research also examines the weaknesses of IoT network construction and identifies potential reasons for its susceptibility to DDoS attacks. Furthermore, the article highlights gaps in prior research on DDoS attacks. The promising results of the proposed model demonstrate its potential to effectively secure IoT network systems in real-world scenarios. Nonetheless, the study's primary limitation is the unavailability of a realistic testing platform, which raises questions about testing reliability. Future research will concentrate on identifying the bottlenecks of IoT network systems concerning their susceptibility to DDoS attacks.

Abbreviations

MQTT	:	Message Queuing Telemetry Transport
BS	:	Bootstrap
SDN	:	Software-Defined Networking
ML	:	Machine Learning
RF	:	Random Forest
FPR	:	False Positive Rate
SVM	:	Support Vector Machine
CAIDA	:	Cooperative Association for Internet Data Analysis
KNN	:	K-Nearest Neighbors
CNN	:	Convolutional Neural Network
RNN	:	Recurrent Neural Network
SGD	:	Stochastic Gradient Descent
DoS	:	Denial of service attacks
DDoS	:	Distributed denial of service attacks
IoT	:	Internet of Things
BiLSTM	:	Bidirectional long short-term memory

Conflict of interest: The authors have no conflicts of interest to declare.

Data availability statement: The dataset used for this research is available online and has a proper citation within the article's contents.

REFERENCES

[1] Jianjian, D., Yang, T., & Feiyue, Y. (2018). A novel intrusion detection system based on IABRBFSVM for wireless sensor networks. Procedia computer science, 131, 1113–1121. DOI: 10.1016/j.procs.2018.04.275

[2] Hosseinzadeh, M., Yoo, J., Ali, S., Lansky, J., Mildeova, S., Yousefpoor, M. S., ... & Tightiz, L. (2023). A fuzzy logic-based secure hierarchical routing scheme using firefly algorithm in Internet of Things for healthcare. Scientific Reports, 13(1), 11058. DOI: 10.1038/s41598-023-38203-9

[3] Giotis, K., Apostolaki, M., & Maglaris, V. (2016, April). A reputation-based collaborative schema for the mitigation of distributed attacks in SDN domains. In NOMS 2016-2016 IEEE/IFIP network operations and management symposium (pp. 495–501). IEEE. DOI: 10.1109/NOMS.2016.7502849

[4] Premkumar, M., Ashokkumar, S. R., Jeevanantham, V., Mohanbabu, G., & AnuPallavi, S. (2023). Scalable and energy efficient cluster based anomaly detection against denial of service attacks in wireless sensor networks. Wireless Personal Communications, 129(4), 2669–2691. DOI: 10.1007/s11277-023-10252-3

[5] David, J., & Thomas, C. (2019). Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Computers & Security, 82, 284–295. DOI: 10.1016/j.cose.2019.01.002

[6] Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. IEEE access, 8, 132 502–132 513. DOI: 10.1109/ACCESS.2020.3009733

[7] Mohammed, S. S., Hussain, R., Senko, O., Bimaganbetov, B., Lee, J., Hussain, F., ... & Bhuiyan, M. Z. A. (2018, October). A new machine learning-based collaborative DDoS mitigation mechanism in software-defined network. In 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 1–8). IEEE. DOI: 10.1109/WiMOB.2018.8589104

[8] Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. International Journal of Computer Applications in Technology, 57(4), 312–324. DOI: 10.1504/IJCAT.2018.093533

[9] Zhang, H., Yu, L., Xiao, X., Li, Q., Mercaldo, F., Luo, X., & Liu, Q. (2023). TFE-GNN: A Temporal Fusion Encoder Using Graph Neural Networks for Fine-grained Encrypted Traffic Classification. In Proceedings of the ACM Web Conference 2023 (pp. 2066–2075). DOI: 10.1145/3543507.3583227

[10] Premkumar, M., Ashokkumar, S. R., Mohanbabu, G., Jeevanantham, V., & Jayakumar, S. (2022). Security behavior analysis in web of things smart environments using deep belief networks. International Journal of Intelligent Networks, 3, 181–187. DOI: 10.1016/j.ijin.2022.10.003

[11] Hayyolalam, V., & Kazem, A. A. P. (2018). A systematic literature review on QoS-aware service composition and selection in cloud environment. Journal of Network and Computer Applications, 110, 52–74. DOI: 10.1016/j.jnca.2018.03.003

[12] Garcia, J. F. C., & Blandon, G. E. T. (2022). A deep learning-based intrusion detection and preventation system for detecting and preventing denial-of-service attacks. IEEE Access, 10, 83 043–83 060. DOI: 10.1109/ACCESS.2022.3196642

[13] Catak, F. O., & Mustacoglu, A. F. (2019). Distributed denial of service attack detection using autoencoder and deep neural networks. Journal of Intelligent & Fuzzy Systems, 37(3), 3969–3979. DOI: 10.3233/JIFS-190159

[14] Nguyen, X. H., & Le, K. H. (2023). Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. Internet of Things, 23, 100851. DOI: 10.1016/j.iot.2023.100851

[15] Yin, C., Zhu, Y., Fei, J., & He, X. (2017).A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21 954–21 961. DOI: 10.1109/ACCESS.2017.2762418

[16] Li, Y., Liu, B., Zhai, S., & Chen, M. (2019, April). DDoS attack detection method based on feature extraction of deep belief network. In IOP Conference Series: Earth and Environmental Science (Vol. 252, No. 3, p. 032013). IOP Publishing. DOI: 10.1088/1755-1315/252/3/032013

[17] Farukee, M. B., Shabit, M. Z., Haque, M. R., & Sattar, A. S. (2021). DDos attack detection in iot networks using deep learning models combined with random forest as feature selector. In Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2 (pp. 118–134). Springer Singapore. DOI: 10.1007/978-981-33-6835-4_8

[18] Ye, J., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018. DOI: 10.1155/2018/9804061

[19] Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24), 11634. DOI: 10.3390/app112411634

[20] Aswad, F. M., Ahmed, A. M. S., Alhammadi, N. A. M., Khalaf, B. A., & Mostafa, S. A. (2023). Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. Journal of Intelligent Systems, 32(1), 20220155. DOI: 10.1515/jisys-2022-0155

[21] Saini, P. S., Behal, S., & Bhatia, S. (2020, March). Detection of DDoS attacks using machine learning algorithms. In 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 16-21). IEEE. DOI: 10.23919/INDIACom49435.2020.9083716

[22] Shang, Y., Yang, S., & Wang, W. (2018, June). Botnet detection with hybrid analysis on flow based and graph based features of network traffic. In International Conference on Cloud Computing and Security (pp. 612–621). DOI: 10.1007/978-3-030-00009-7_55

[23] Yousuf, O., & Mir, R. N. (2022). DDoS attack detection in Internet of Things using recurrent neural network. Computers and Electrical Engineering, 101, 108034. DOI: 10.1016/j.compeleceng.2022.108034

[24] Alshehadeh, A. R., & Al-Khawaja, H. A. (2022). Financial Technology as a Basis for Financial Inclusion and its Impact on Profitability: Evidence from Commercial Banks. Int. J. Advance Soft Compu. Appl, 14(2). DOI: 10.15849/IJASCA.220720.09

[25] Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., ... & Bajandouh, S. A. (2023). DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. Electronics, 12(14), 3103. DOI: 10.3390/electronics12143103

[26] UNB 2017 Intrusion Detection Evaluation Dataset by canadian institute for cybersecurity URL. https://www.unb.ca/cic/datasets/ids-2017.html

Iqbal Jebril comleted his Ph.D. (Mathematical Analysis) Universiti Kebangsaan National University of Malaysia. He is working as professor and Head of the Mathematics Department, Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, P.O. Box 130 Amman 11733 Jordan

M. Premkumar received the Ph.D. degree in Information and Communication Engineering from Anna University Chennai in 2022. His research interests include wireless Ad hoc networks, security and key management of wireless networks, wireless sensor networks.

Ghaida Muttshar Abdulsahib working as a faculty in computer engineering department, University of Technology, Iraq. She got a lot of awards in computer engineering area. And now Ghaida interested in network and communication area. She also published articles in reputed indexed journals like SCI, WoS and SCOPUS.

S. R. Ashokkumar received the Ph.D. degree in Information and Communication Engineering from Anna University Chennai in 2021. His research interests include Network security and Signal and image processing, wireless sensor networks.

S. Dhanasekaran received his BE degree in Electronics and Communication Engineering in 2008 from Sri Balaji Chockalingam Engineering College, Arani, Tamil Nadu, India. He completed his ME in Communication Systems in 2010 from PSG College of Technology, Coimbatore, Tamil Nadu, and India. He completed his PhD in the year 2022 from Anna University Chennai in the area of Communication systems, MIMO, OFDM, etc.,

He is currently working as Assistant Professor in the department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore. He has around 14 years of teaching experience. He is a life time member of ISTE.

Osamah Ibrahim Khalaf is a Senior Engineering and Telecommunications Lecturer in Al-Nahrain University / College of Information Engineering. He has had many published articles indexed in (ISI/Thomson Reuters/SCI) and has also participated and presented at numerous international conferences. In 2004, he got his B.Sc. in software engineering field from Al-Rafidain University College in Iraq. Then in 2007, he got his M. Sc. in computer engineering field from Belarussian National Technical University. After that, he got his Ph.D. in 2017 in the field of computer networks from faculty of computer systems and software engineering, University Malaysia.

Sameer Saadoon Algburi, got the PhD in 2007 from the University of Technology in Iraq in electrical power systems. A Professor at Al-Kitab University in Kirkuk in teaching undergraduate students and supervised graduate students. interested in power systems, especially renewable energies and climate change and published many papers in local and international conferences and journals. Since 2014, Visiting Researcher at two Lund University centers, the Geographic Information Center GIS and the Center for Middle Eastern Studies CMES. Since 2019, Director and founder of the Swedish-Iraqi Studies Network SISNET and managed it with the help of two boards of management and consulting from Iraq and Sweden. UN/ UNIDO, China, Small Hydropower Systems, Author and UN/ UNIDO/CTCN member. Also the Managing Editor at Al-Kitab Journal for Pure