THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 1 (2024)
https://doi.org/ 10.62019/abbdm. v4i1.113.

Effective Intrusion Detection System Using Deep Learning for DDoS Attacks

Jahangir Shaikh*, Yasir Awais Butt, Hira Fatima Naqvi

Chronicle

Article history

Received: February 15, 2024
Received in the **revised format:** Feb 22, 2024
Accepted: Feb 25, 2024
Available online: Feb 29, 2024

Jahangir Shaikh and Yasir Awais Butt are currently affiliated with Abasyn University Islamabad, Pakistan.
Hira Fatima Naqvi is affiliated with University of Sindh Jamshoro, Sindh, Pakistan.
Email:jahangir.shaikh.dsu@gmail.com
Email:yasir.awais@abasynisb.edu.pk
Email:hira.naqvi@usindh.edu.pk

Corresponding Author*

Abstract

An increasing demand for information technology and cloud computing has led to various security threats over internet. Amongst all types of threats, Distributed Denial of Service (DDoS) attacks are the most common, posing a challenge to a cyber security. It allows unauthorized users to gain access to services, and preventing authorized users. Traditional intrusion detection, antivirus software, and firewalls are not enough to detect these attacks. This paper proposed an efficient deep learning-based intrusion detection system (IDS) for DDoS attacks detection. Proposed model is a hybrid CNN-LSTM model which is combination of best DL algorithms to take advantage of CNN to extract spatial features and LSTM to extract temporal features. The real-time DDoS-specific benchmark-dataset CICDDoS2019 used for training, testing, and validation. An autoencoder has been used for dimensionality reduction, and SMOTE method is used to balance the minority class of dataset. The experimental results proved that the model outperforms than other state-of-the-art models, with an accuracy score of 99.86%.

Keywords: DDoS, IDS, LSTM, CNN, SMOTE, Autoencoder, DL

INTRODUCTION

The internet has transformed the way of communication, conducting and interacting with business, and carrying out day-to-day operations. Internet services have been integrated into traditional sectors like research, education, banking, defense, medicine, and entertainment. Data is now considered a more valuable resource than oil (Oman, n.d.). The volume of data transferred on the internet continues to grow, and like any resource, it is prone to various security hazards. The public and private sectors have huge investments in IT, which has raised the demand for data security. According to the author (Macas et al., 2020), there will likely be more IP-connected devices by 2023, which can generate a large volume of IP traffic, posing major security concerns. Consequently, the importance of cyber security tools, experts, and practices has increased manifold. Cybercriminals are always devising new strategies to bypass security and evade detection. Because cyber attackers use creative approaches and advanced practices, there is a continuing need to update the field of cyber security technologies at a commensurate rate. The most widespread security concern in the present digital world is distributed denial of service (DDoS) attacks (Yuan, Li et al., 2017). DDoS attacks can have severe and wide-ranging impacts on both individuals and organizations. Some key aspects of the severity and impact of DDoS attacks are Disruption of Services, Financial Losses, Reputation Damage, Data Breach Risks, Collateral Damage, and Impact on

Critical Infrastructure. The main objective of DDoS attacks is to deplete network resources to prevent applications from providing services to legitimate users. DDoS attacks originate when hostile actors bombard the hosting server with a lot of unnecessary traffic to keep it busy serving undesired requests. Resulting in the ultimate overwhelming of illegal traffic, and the actual user is unable to connect and be served. Therefore, the need for a reliable means of identifying DDoS attacks has increased (Alanazi et al., 2022). Traditional antivirus software and firewalls are not enough. Subsequently, an effective intrusion detection system (IDS) is required to detect DDoS attacks (Das et al., 2019). IDS is important in the cyber security environment for improving protection against developing threats like DDoS attacks. The introduction of artificial intelligence (AI) has transformed IDS. AI is further subdivided into machine learning (ML) and deep learning (DL). Manual feature extraction is used in ML, whereas DL uses neural networks to extract features automatically.

DL, a popular AI subset, is widely used in IDS due to its ability to detect detailed patterns linked to cyber threats. The DL-based hybrid CNN-LSTM model is also being used to detect DDoS attacks (Rajakumaran et al., 2020). It has gained prominence in a variety of fields, including speech recognition, image processing, language translation, and IDS (Yuan et al., 2019). The latest developments in explainable AI (XAI) have increased the dependability of DL-based IDS models, allowing for in-depth analysis and predictability. This AI-IDS synergy not only solves shortcomings in previous techniques but also drives the ongoing refining of IDS for strong cyber security (Nwakanma et al., 2023). The authors (Laghrissi et al., 2021) created an LSTM model to predict network attacks using the KDD99 dataset. The outdated dataset does not include the most recent malicious traffic. Therefore, an isolated DL model may be less successful in predicting DDoS attacks.

To resolve these concerns, this study adopts a DL-based hybrid model for detecting DDoS attacks that increases an IDS's efficiency. The suggested model is a hybrid of an LSTM for sequence prediction and a CNN for extracting features from input (Rusyaidi et al., 2022). The proposed model was trained and assessed using the CICDDoS2019 DDoS-specific datasets (DDoS 2019, n.d.). The model recognizes spatial and temporal patterns, which results in a lower FAR and a higher accuracy score. Experiment findings show that combining these two DL algorithms improves the accuracy of an IDS. Various studies on the DL-based hybrid model have already been conducted; however, the novelty of this research is the use of the SMOTE method to resolve class imbalance and an autoencoder for dimensionality reduction of the CICDDoS2019 dataset to increase the efficacy and sensitivity of the DL-based CNN-LSTM model, which improved the overall effectiveness of an IDS to detect DDoS attacks. The main contribution of this research work are manifold:

- To analyze the DDoS-specific CICDDoS2019 dataset and its features to check for any redundancies that may affect prediction results and to remove all null or ambiguous values.
- To create a hybrid DL-based CNN-LSTM model that can accurately recognize DDoS attacks by combining CNN with LSTM to learn spatial and temporal features from input data.
- To enhance the model's accuracy by using SMOTE to resolve the class imbalance and an autoencoder for dimensionality reduction to overcome the issue of computing requirements.

- To compare the performance of the model with other state-of-the-art models and evaluate proposed model in terms of precision, recall, F1-score and accuracy.

The further organization of the paper will be as follows: Section 2 presents the background. Section 3 outlines the literature review. Section 4 describes the Material and Methods Section 5 discuss the methodology of the proposed model. Experimental results are explained in Section 6, whereas Section 7 describes the discussion and limitations. Section 8 includes the conclusion and future work.

BACKGROUND

Intrusion Detection System Overview

An IDS is a software or hardware that detects malicious activity on computer networks. The primary purpose of an IDS is to ensure the security of computer systems by detecting and identifying various forms of malicious network traffic and device usage that may evade traditional firewalls. It is a crucial component of cyber security systems, designed to detect cyber threats while ensuring user access and privacy protection. IDS collects and analyzes data to identify potential threats, providing valuable insights for security analysts. There are two detection approaches to an IDS, i.e., misuse and anomaly detection. IDS can be categorized as network-based or host-based (Karatas et al., 2018). Deep learning approaches are widely utilized as part of artificial intelligence (AI) in an IDS.

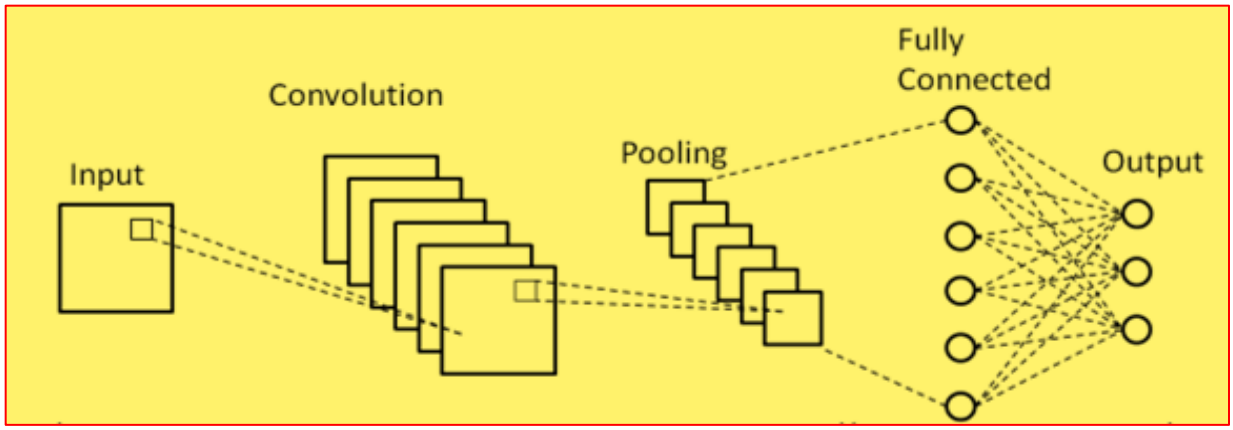
DL-Based IDS

ML can be subdivided into shallow and deep learning; DL involves the utilization of multi-hidden-layer ANN. Unlike ML, DL algorithms can learn from unstructured or unlabeled data. DL algorithms exhibit several performance features that make them suitable for developing an IDS. DL algorithms are known for their robustness, scalability, and adaptability to different datasets (Edeh et al., 2021). Initially, it was developed to address multifarious problems like machine translation and pattern recognition. DL techniques have gained prominence. CNNs are widely used due to their automatic spatial feature recognition, capacity to prevent overfitting by reducing trainable parameters, and improved generalization (Vigneswaran et al., 2018). On the other hand, LSTM finds applications in natural language processing as it effectively captures sequential network features. It was specifically developed to overcome the vanishing gradient problem encountered in RNN due to its memory blocks (Shi et al., 2020).

Convolutional Neural Network

A CNN is an ANN with convolutional, pooling, and fully connected layers. Together, these layers help the raw data be transformed into informative representations. In Figure. 1, the convolutional and pooling layers process the input at first, creating different feature maps to identify significant patterns in the data. A completely linked layer receives the output of these layers and performs classification on it. Gradient descent is used during training to optimize the weight parameters of the convolutional and fully connected layers. The benefit of automatic feature extraction is one that CNN offers, and it has grown in favor in recent studies. To make the 1D input compatible with the network's 2D structure, additional preprocessing could be necessary when utilizing CNN in the context of 2D

data, such as photos. For example, (Jia et al., 2020) presented a unique CNN architecture created especially for DDoS detection on datasets like KDD99, private datasets, and



CICDoS2019.

Figure 1.
CNN Architecture

Long Short-Term Memory

The LSTM is an extension of RNN. While RNNs struggle with learning long-term dependencies, LSTMs have been developed to overcome this limitation. LSTMs have demonstrated the ability to capture long-term dependencies while preserving their ability to process short-term information efficiently. Unlike RNNs that have simply hidden layers composed of tanh units, LSTM architectures consist of four hidden layers, as depicted in Figure 2. The input gate, output gate, and forget gate are three gates that are incorporated into LSTM. Memory cell is an essential component of LSTM. It is made up of linked neurons that remember past inputs and preferentially forget them periodically to deal with new information (Hochreiter et al., 1997). LSTM gates are as under:

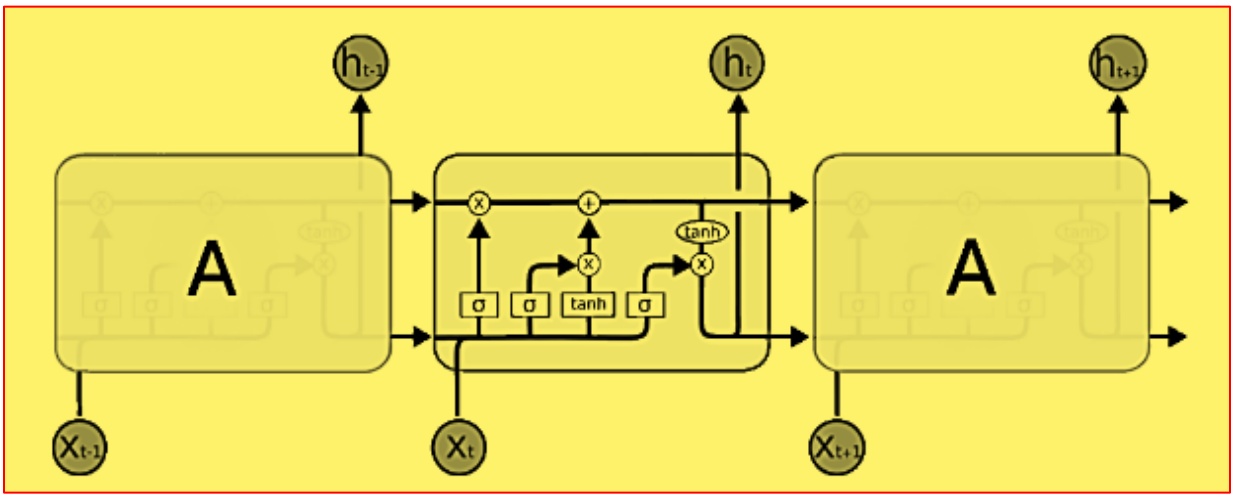


Figure 2.
LSTM Architecture (Laghrissi et al., 2021)

Input Gate: It is responsible for regulating the amount of new information from current input that will be saved in a cell.

$$I_t = \sigma(w_{\mathrm{i}} * [h_{t-1}, x_t] + b_i) \quad (1)$$

$$C_t = \tanh(w_c * [h_{t-1}, x_t] + b_c) \quad (2)$$

Output Gate: It is responsible for deciding the part of a cell state that will be output to the next hidden state.

$$o_t = \sigma(w_o * [h_{t-1}, x_t] + b_o) \quad (3)$$

Forget Gate: It is responsible for determining the amount to which the preceding cell state must be forgotten or discarded.

$$f_t = \sigma(w_f * [h_{t-1}, x_t] + b_f) \quad (4)$$

Cell State: It represents the new information that could be stored in the cell state.

$$C_t = f_t * C_{t-1} + i_t * \mathbb{C}_t \quad (5)$$

Hidden State: Output of the LSTM cell, which contains information that can be passed to the next step or for prediction.

$$h_t = o_t * \tanh(C_t) \quad (6)$$

LITERATURE REVIEW

Research community has introduced various DDoS detection and mitigation strategies. This section provides a brief overview of the existing strategies that employ DL for DDoS detection. Various studies suggested schemes for DDoS detection based on traditional ML and DL models. However, Omer Aslan (Aslan, 2022) provided a strategy for identifying DDoS attacks using the CICDDoS2019 dataset. This methodology centers on applying various methods to reduce dimensionality. Gain Ratio and RF were used in the study to attain 99% accuracy, whereas other classifiers like KNN and AdaBoost had lower accuracy rates. Three DL-based algorithms, LSTM, RNN, and CNN, were merged by (Aswad et al., 2023) to create a CNN-BiLSTM to detect DDoS attacks using the CICIDS2017 dataset. CNN displayed an accuracy score of 98.82%, while RNN and LSTM each achieved 99.00%. The authors recommend contrasting their model with different DL models. DDoS attack detection using a hybrid DL-based CNN-BiLSTM model was proposed by (Alghazzawi et al., 2021). Utilizing the CICDDoS2019 datasets to evaluate their model, the researcher outperformed competing models and achieved an accuracy of 94.52%.

An efficient DL-based method to detect DDoS attacks was proposed by (Lopes et al., 2021). They used DNN and ML classifiers in an ensemble to select features. The CICDDoS2019 dataset was used to train the model, which quickly demonstrated high DDoS attack prediction accuracy. The model, however, was only capable of binary classification. To improve the accuracy of an IDS, (Zhang et al., 2019) developed a DL-based hybrid model that combines LSTM and CNN. It passes the extracted features from the CNN layer to the LSTM layer. The hybrid model used the CICIDS2017 dataset, and it achieved a high F1 score for binary classification (99.88%), outperforming the standalone

LSTM and CNN models. However, for multiclass classification, the CNN model achieved a higher F1 score of 99.9%. (Ramzan et al., 2023) adopt a DL-based model including LSTM, RNN, and GRU for DDoS attacks detection with DDoS specific CICDDoS2019 and CICIDS2017 datasets. It performs well on the CICDDoS2019 dataset and produces a 99.9% result, where GRU takes less time than LSTM and RNN. (Gaur et al., 2022) used the M-LSTM model for DDoS attack detection and achieved precision, recall, and F-1 scores of 98.75%, 97.5%, and 98%, respectively, by using the CICDDoS2019 dataset. According to (Elsayed et al., 2021), combining CNN with LSTM produces 96.32% accuracy, showing the efficacy of the hybrid model for an IDS. This approach beats all other algorithms. For an improved intrusion detection system, a hybrid deep learning (HDL) network made up of CNN and LSTM is employed in the suggested system (Vinayakumar et al., 2017). The UNS-NB15 dataset served as the basis for the binary classification assessment. Thus, in terms of binary classification, the suggested strategy has achieved 99.17% accuracy. (Issa et al., 2023) used a novel DL classification model with two common DL algorithms, CNN and LSTM, with the NSL-KDD dataset and achieved an accuracy of 99.20%. (Amrish et al., 2022) used various ML and DL models for DDoS attack detection using the CICDDoS2019 dataset and produced accuracy score of 99.95% using the ANN.

The choice of dataset for evaluating a DL-based IDS is crucial in assessing its effectiveness in identifying potential DDoS attacks. Many existing DL-based strategies fail to detect recent attacks highlighted by researchers, due to the constraints of the datasets used for training and evaluation. Conversely, some recent studies do take into account datasets that include data pertaining to recent DDoS attacks. However, these studies involve high computational overhead for training the models and making predictions. The computational complexity of the detection system can be substantially reduced if the number of features used for training and detection can be minimized without compromising the IDS performance. To address these issues, we suggest a hybrid DL-based model that achieves superior DDoS attack detection accuracy and demands less computational resources compared to its peers. Moreover, the difference between the majority class and the minority class also affects the accuracy of the model. A useful dataset with efficient preprocessing steps is required to increase the efficacy and sensitivity of the model which improves the overall effectiveness of an IDS to detect DDoS attacks.

MATERIAL AND METHODS

Dataset

The well-known DDoS-specific CICDoS2019 dataset, released by the Canadian Institute for Cybersecurity and available on their website (DDoS 2019, n.d.), is utilized in the proposed model. The motivation behind choosing the CICDDoS2019 dataset lies in its relevance and suitability for evaluating DDoS detection techniques. The dataset is significant in the context of DDoS detection for several reasons. Overall, the CICDDoS2019 dataset serves as a valuable resource for advancing research and innovation in DDoS detection and cybersecurity. Its realistic attack scenarios, diverse attack types, high-quality features, large-scale dataset size, and benchmarking capabilities make it a compelling choice for evaluating and improving the effectiveness of DDoS detection techniques in real-world network environments. The dataset details

are shown in Table 1, which includes benign and wide-ranging DDoS attacks. IDS in DL heavily relies on the availability of datasets. However, the scarcity of such datasets is due to privacy and regulatory concerns regarding the sensitive information present in network traffic. To overcome this challenge, researchers often resort to creating simulated data. However, these simulated datasets often lack completeness and do not adequately cover the range of application behaviors. Several public domain datasets have been widely used for an IDS to overcome this issue. There are primarily two kinds of attacks. Reflection-based: a response-based authentication scheme that follows the same protocol everywhere. It is made up of NetBIOS, TFTP, and DNS types. Another type of attack is called exploitation-based when an attacker attempts to use a weak system to hurt themselves. It is made up of UDPLag, UDP, and SYN. This dataset was chosen primarily because it is one of the most recent in the IDS area for identifying DDoS attacks and has a lot of potential for future research applications. There are around 50 million data points in the dataset. A total of 4.4% of records were selected, i.e., 2.2 million data records from the dataset (2 lacs from 11 classes), due to the limitations of computational resources.

Table 1.
CICDDoS2019 Dataset

Type	Total
Benign_	56863
LDAP_	2179930
TFTP_	20082580
DNS_	5071011
NetBIOS_	4093279
MSSQL_	4522492
SSDP_	2610611
NTP_	1202642
SNMP_	5159870
UDP_	3134645
SYN_	1582289
UDP-Lag_	366461
WebDDoS_	439
Total	50063112

DATASET PREPROCESSING

The data preparation stage includes the elimination of all nulls and outliers, normalization, dimensionality reduction, and addressing class imbalance issues. To prepare the dataset to train the model, certain features were identified and deleted, like SimillarHTTP, Flow ID, Source Port, Unnamed: 0, Source IP, Destination IP, Timestamp, Destination Port, and Label, due to not being suitable for training. To further preprocess the dataset, the following common data preprocessing steps were applied:

Data Cleaning

One of the most important steps in reducing noise and improving the overall quality of the data is to remove duplicate, NaN, or irrelevant data points from the dataset. Furthermore, there were 12 features i.e. Idle Std, Max, Mean, Min, Inbound, min_seg_size_forward, act_data_pkt_fwd, Active Std, Min, Mean, Max, and Init_Win_bytes_backward had extremely low variance were eliminated. Eliminating such records enhances the model's performance and decreases computing complexity.

Label Encoding

The label encoding method is used to convert categorical data to numerical data using Sklearn package named Label Encoder. The model was trained to discriminate between legitimate and malicious input traffic to conduct binary classification. All DDoS groups were therefore viewed as attacks. The labels for attack and normal traffic were encoded as binary values of 1 and 0, respectively.

Dimensionality Reduction

Dimensionality reduction involves the selection of features by certain standards. This is very crucial in enabling the construction, training, and test model, as it focuses on essential features. It decreases the time for both training and testing to improve overall performance. (Wei et al., 2021) in his research stated that an autoencoder AE identifies the most significant features automatically. In this research, an AE technique has been used. It is an unsupervised deep learning method that involves encoding and decoding the original data to reduce the dimensions. The encoding layers transform the data into a lower-dimensional space to capture the most informative features, while the decoding layers reconstruct the data from this space in an unsupervised manner. The dimension of the dataset was reduced to 30 features based on the variance and eigenvalues.

Class Imbalance

Class imbalance is a severe problem in ML and DL models, resulting in biased outputs with high FPRs when model is trained on imbalance dataset. Under-sampling and over-sampling approaches are commonly utilized to solve this issue. In this study, SMOTE (synthetic minority oversampling) is employed to solve the issue of class imbalance. SMOTE was first proposed by (Chawla et al., 2002). It is especially useful when working with datasets when the majority class (DDoS attacks) outnumbers the minority class (normal traffic). SMOTE's main objective is to produce synthetic cases for the minority class to balance the dataset and provide more representative training data to the model. SMOTE is an effective strategy for dealing with imbalanced classes.

Overfitting and Regularization

Overfitting is a severe problem in neural networks that occurs when a neural network model works well on training data but not on test data. This is because the model was trained on inaccurate information, such as outliers. There are numerous approaches of dealing with such issues. Although the method has limitations with datasets availability, increasing the quantity of training data is a popular technique for reducing overfitting. Another option is to employ regularization techniques to penalize heavier weights. To improve the model and enable lower weights, a variety of regularization procedures, such as L1 and L2, can be utilized. In addition to the regularization approaches described above, dropout is a commonly used tool to reduce the chance of overfitting.

Dataset Split

Maintaining a balanced dataset is crucial for both training and testing the model, as it can affect the results. There are training and testing datasets inside the CICDDoS2019.

Data splitting is done using the Sklearn library. 30% of the data is used for testing and validation, while 70% is used for training.

METHODOLOGY

The study proposed a DL-based hybrid CNN-LSTM to predict DDoS attacks with CICDDoS2019 dataset for binary class classification. The decision to use hybrid DL-based CNN-LSTM model is typically motivated by the desire to harness the advantages of both CNN and LSTM. CNNs excel at processing spatial information and are commonly used in image recognition tasks, while LSTMs are designed to handle temporal information, making them ideal for tasks involving sequential data, such as natural language processing or time-series prediction. By combining these two, the model can effectively process data with both spatial and temporal dimensions. In this model, initially, the data passes through the CNN layer. Within the convolution layer, filters are employed to extract the most important features, resulting in the generation of a feature map, and then go through max pooling layer. After CNN, output is fed to the LSTM layer to extract temporal data, A dropout layer is applied to avoid overfitting, and finally, a sigmoid activation function is used to classify between DDoS and normal traffic. To get the best performance, the dataset needs to be in the right format for training. The preparation of the dataset is done, and it takes multiple steps. To improve the training of the models and lessen ambiguity in the data, missing and null values are eliminated. 30 features with highest eigenvalues are chosen at the data preprocessing stage by using Autoencoder for dimensionality reduction. Reducing dimensionality in models aims to improve their performance in terms of accuracy and sensitivity rates while using less computational resources. Figure 3 describes the proposed DL-based hybrid CNN-LSTM model. The model provides a powerful framework for capturing both spatial and temporal dependencies in data, leading to improved performance and accuracy compared to using CNNs or LSTMs independently.

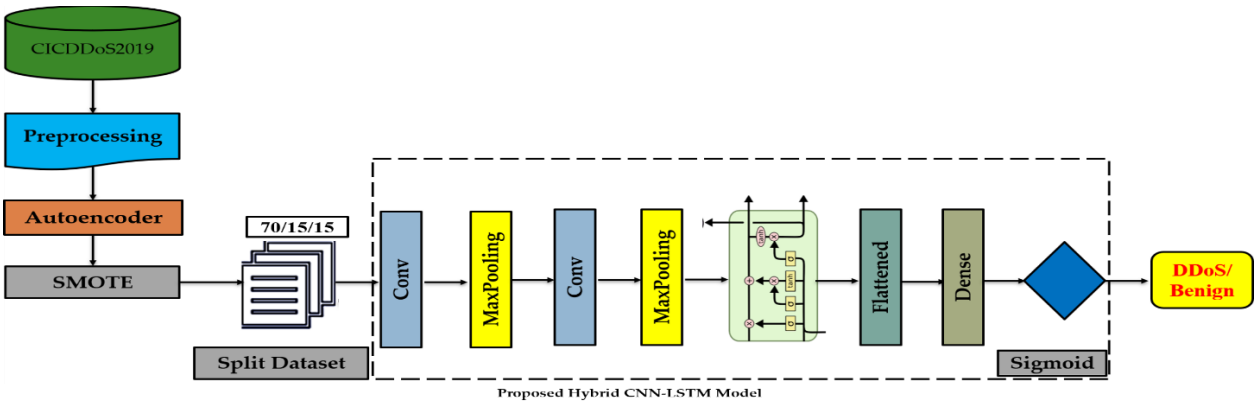


Figure 3.
DL-Based Hybrid CNN-LSTM Model

Hyperparameter tuning involves selecting the optimal values for parameters that are not learned during training instead they are set before training begins. The hyperparameters used in this model are shown in Table 2. Here is an overview of how hyperparameters are tuned and the rationale behind the chosen values.

Learning Rate: A higher learning rate may lead to faster convergence but risk overshooting the optimal solution, while a lower learning rate may converge more slowly but offer better stability. The learning rate of proposed model is 0.0001.

Batch Size: Larger batch sizes can speed up training but may require more memory and lead to poorer generalization, while smaller batch sizes may offer better generalization but slower training. In this research batch size is taken as 512.

Number of Layers and Units: The number of layers and units in a neural network architecture depends on the complexity of the problem and the amount of available data.

Regularization Strength: Regularization techniques such as L1 or L2 regularization and dropout are used to prevent overfitting by penalizing large weights or randomly dropping units during training. L2 regularization has been used in the proposed model. Overall, hyperparameter tuning is an iterative process that involves experimenting with different hyperparameter configurations, evaluating their performance through cross-validation, and selecting the values that yield the best results.

Table 2.
Hyperparameters

Parameter	Value
Activation Function	Relu and Sigmoid
Loss Function	binary_crossentropy
Optimizer	RMSprop
Learning Rate	0.0001
Epochs	5
Dropout	0.2
Regularization	L2
Dimensionality Reduction	Autoencoder/PCA
Class Imbalance	SMOTE
Batch Size	512
Training Split	70/15/15

EVALUATION AND RESULTS

Experimental Environment

The proposed model was evaluated on an Intel Core i3-1115 G4 processor at 3.0 GHz, 16 GB of RAM, and the Windows 11 operating system with python programming language version 3.11.4 with some libraries like Keras (2.13.1), Sklearn (1.3.0), Numpy (1.24.3), Pandas (2.0.3), and Matplotlib (3.7.2).

Evaluation of model and Evaluation Criteria

In this study, the effectiveness of the model has been evaluated using various metrics, like accuracy, precision, F1 score, sensitivity or recall, and time. Table 3 provides a detailed overview of the confusion matrix, offering a comprehensive summary of the classification results. The evaluation metrics are as follows:

Table 3.
Confusion matrix

	Positive	**Negative**
Positive	TP	FP
Negative	FN	TN

TP: It represents the correctly detected attacks.

FP: It represents the incorrectly detected normal traffic as attacks.

TN: It represents the correctly detected normal traffic.

FN: It represents the incorrectly detected attacks as normal traffic.

These metrics are calculated using the following mathematical equations:

Precision: It measures the ratio of correctly predicted attacks by all data categorized as attacks.

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

Accuracy: It measures the ratio of correct predictions to the total predictions.

$$Accuracy = \frac{TN+TP}{TP+FP+TN+FN} \quad (8)$$

F1Score: It is the combination of precision and recall and is calculated by the harmonic mean of precision & recall.

$$F1 - Score = \frac{2*P*R}{P+R} \quad (9)$$

Sensitivity or Recall: It is also called TPR true positive rate, it measures the ratio of correctly predicted attacks by all actual attack instances.

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

Training time: It represents the time taken by the model during training.

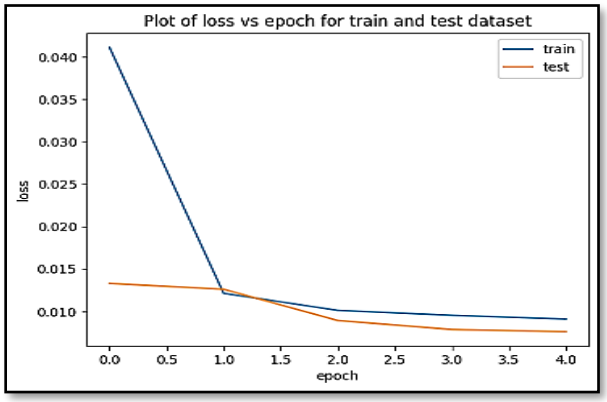
EXPERIMENTAL RESULTS

The model performance was compared with individual LSTM and CNN models by using 30, 20, and 10 features. 200000 data samples were taken from each class of the CICDDoS2019 dataset, which makes 2.2 million data points. Initially, the data was imbalanced, so the SMOTE technique was used to balance the normal and DDoS traffic in the dataset, resulting in 4.4 million data points. The maximum accuracy of the proposed model was achieved with 30 features, an autoencoder, and binary classification at **99.86%**, as mentioned in Table 4. Accuracy and loss curves can be seen in Figure 4, whereas the confusion matrix is in Figure 5. However, it's important to note that while conducting a cost-and-benefit analysis, there is always a trade-off between accuracy and resources (Khattak et al., 2022).

Table 4.

Result

Model	Acc	Precision	Ser
LSTM	99.42	99.3	99.
CNN	99.75	99.9	99.
CNN-LSTM	**99.86**	**99.9**	**99.**



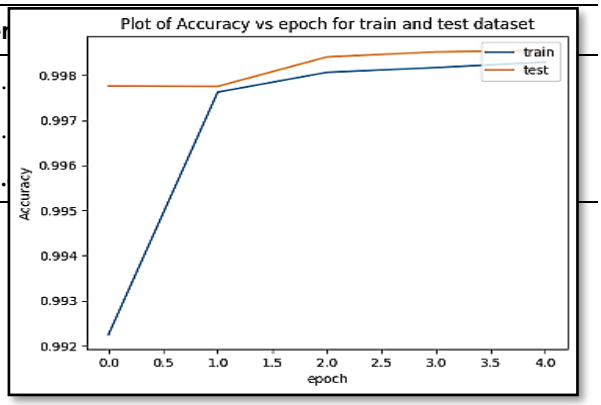


Figure 4.
Accuracy and Loss Curve

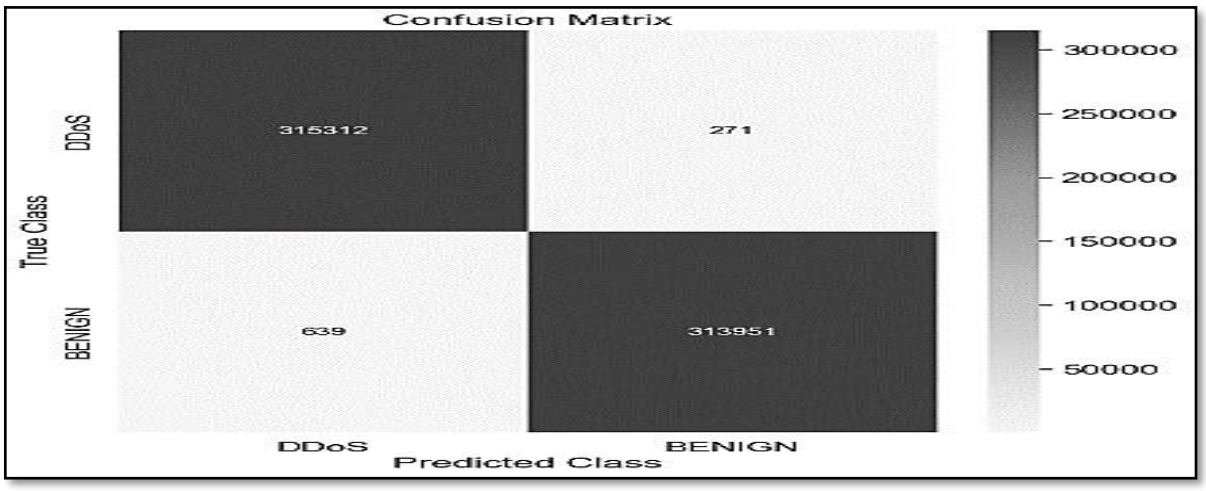


Figure 5.

Confusion Matrix

Table. 5

Title	Model	Accuracy
Proposed: "Effective IDS using deep learning for DDoS"	**CNN-LSTM**	**99.86**
(Zainudin et al., 2022) "A Lightweight Deep Learning-based Anomaly Detection and Classification in Software-Defined Industrial Network"	CNN-LSTM	99.02
(Alghazzawi et al., 2021) "Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection"	CNN-BiLSTM	94.52

(Mahadik et al., 2022) "Edge-HetIoT Defense against DDoS attacks using Learning techniques"	CNN-LSTM	92.00
(Kumar et al., 2023) "DDoS Detection using Deep Learning"	LSTM	98.00
(Badamasi et al., 2020) "A Deep Learning based approach for DDoS attack detection in IoT-enabled smart environments"	LSTM	99.60
(Wahab et al., 2022) "An AI-Driven Hybrid Framework for Intrusion Detection in IoT-Enabled E-Health"	LSTM-GRU	99.01
(Shieh et al., n.d.) "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric"	CNN	99.80

Comparison with other state-of-the-art models

DISCUSSION AND LIMITATION

The key objective of this research is to develop an effective IDS capable of accurately distinguishing between normal and DDoS attack traffic. The increasing complexity of cyber security issues and the rising number of new attacks pose challenges for traditional IDS, which often suffer from a high false alarm rate. This high FAR leads to security experts disregarding potentially harmful attacks, leaving the system vulnerable. To address these limitations, researchers have recently turned to DL-based approaches for an IDS. Recent studies have shown that DL models outperform conventional techniques in detecting malicious traffic and classifying DDoS attacks. Many researchers have separately utilized CNN and LSTM configurations, whereas this model takes a hybrid approach. In this hybrid model, both CNN and LSTM are combined. This integration of CNN and LSTM enhances the model's ability to effectively analyze and classify the data. The hybrid DL-based CNN-LSTM model was adopted because of its architecture, which combined the use of convolutional processes to extract spatial patterns with CNN and the LSTM's to grasp temporal correlations. The model can simulate temporal correlations that are essential for binary classification. The proposed hybrid DL-based CNN-LSTM model's architecture has successfully achieved the main objective of obtaining higher accuracy and sensitivity than other models, which shows the efficacy of the proposed model. It demonstrated exceptional performance by achieving an accuracy score of 99.86% for binary classification with 5 epochs. Additionally, the sensitivity score is 99.8%, further highlighting the model's accuracy and reliability as compared to the isolated CNN and LSTM models. The comparison of the proposed model with state-of-the-art approaches in terms of accuracy is illustrated in Table 5.

CONCLUSION AND FUTURE WORK

The Internet has faced numerous malicious intrusions, including DDoS attacks. Detecting DDoS attacks has become increasingly challenging due to evolving network behavior and attack patterns, particularly when using traditional intrusion detection methods. To overcome this challenge, this research developed a unique approach called the DL-based hybrid CNN-LSTM model. Autoencoder is used for dimensionality reduction, and SMOTE is used to balance the dataset. The DDoS-specific CICDDoS2019 dataset is utilized in this model. Feature extraction reduces the number of attributes from 86 to 30. The investigational findings proved that the proposed model performs better than individual CNNs or LSTMs and achieved an accuracy of 99.86%. Overall, the proposed models outperform existing benchmarks and previous studies. However, this thesis acknowledges the ongoing difficulty in detecting DDoS attacks, which continue to pose a significant threat to networks. Despite the extensive efforts made by researchers, DDoS threats and

challenges will persist in the future. Therefore, each researcher's contribution, no matter how small, can make a difference in this field. In this research, it is found that the proposed model has high accuracy with a low FAR for DDoS attacks. The DDoS-specific CICDDoS2019 dataset is used in this model. It is recommended to apply this model to various other datasets in the future. To further increase attack detection, ablation study analysis will be carried out in the future by adding and removing layers from the model. Additional classifiers and variants of CNN and LSTM could be implemented. It has been noted in the literature that finding the right number of hyperparameters for DL models is quite challenging. Therefore, our main focus will be on optimization of hyperparameters and model performance will be further improved by adding multiclass classification for the several types of attacks.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A., & Alsubhi, K. (2022). Ensemble deep learning models for mitigating DDoS attack in software-defined network. Intelligent Automation & Soft Computing, 33(2), 923–938. doi:10.32604/iasc.2022.024668

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 (Basel, Switzerland), 11(24), 11634. doi:10.3390/app112411634

Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A., & Vinoth Kumar, C. (2022). DDoS Detection using Machine Learning Techniques. Journal of ISMAC, 4(1), 24–32. doi:10.36548/jismac.2022.1.003

Aslan, Ö. (2022). A Methodology to Detect Distributed Denial of Service Attacks. Bilişim Teknolojileri Dergisi, 15(2), 149–158.

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). doi:10.1515/jisys-2022-0155

Badamasi, U. M., Khaliq, S., Babalola, O., Musa, S., & Iqbal, T. (2020). A deep learning based approach for DDoS attack detection in IoT-enabled smart environments. International Journal of Computer Networks and Communications Security, 8(10), 93–99.

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. The Journal of Artificial Intelligence Research, 16, 321–357. doi:10.1613/jair.953

Das, S., Mahfouz, A. M., Venugopal, D., & Shiva, S. (2019). DDoS intrusion detection through machine learning ensemble. 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE.

Edeh, D. I. (2021). Network intrusion detection system using deep learning technique.

Elsayed, M. S., Le-Khac, N. A., Jahromi, H. Z., & Jurcut, A. D. (2021). A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 17–20). Vienna, Austria: ARES 2021.

Gaur, M. V., & Kumar, R. (2022). M-LSTM: Multiclass Long Short-Term Memory based approach for Detection of DDoS Attacks. Mathematical Statistician and Engineering Applications, 71(3s2), 1375–1394.

Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780. doi:10.1162/neco.1997.9.8.1735

Issa, A. A., & Albayrak, Z. (2023). Ddos attack intrusion detection system based on hybridization of cnn and lstm. Acta Polytechnica Hungarica, 20(2), 105–123.

Jia, Y., Zhong, F., Alrawais, A., Gong, B., & Cheng, X. (2020). FlowGuard: An intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet of Things Journal, 7(10), 9552–9562. doi:10.1109/jiot.2020.2993782

Karatas, G., & Sahingoz, O. K. (2018). Neural network based intrusion detection systems with different training functions. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE.

Khattak, A., Bukhsh, R., Aslam, S., Yafoz, A., Alghushairy, O., & Alsini, R. (2022). A hybrid deep learning-based model for detection of electricity losses using big data in power systems. Sustainability, 14(20), 13627. doi:10.3390/su142013627

Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS Detection using Deep Learning. Procedia Computer Science, 218, 2420–2429. doi:10.1016/j.procs.2023.01.217

Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(1). doi:10.1186/s40537-021-00448-4

Lopes, O., Zou, I., Ruambo, D., Akbar, F. A., & Yuan, S. (2021). Towards effective detection of recent DDoS attacks: A deep learning approach. Security and Communication Networks, 2021, 1–14.

Macas, M., & Wu, C. (2020). Review: Deep learning methods for cybersecurity and intrusion detection systems. 2020 IEEE Latin-American Conference on Communications (LATINCOM). IEEE.

Mahadik, S. S., Pawar, P., & Muthalagu, R. (2022). Edge-HetIoT Defense against DDoS attack using LearningTechniques. doi:10.21203/rs.3.rs-2164979/v1

Nwakanma, C. I., Ahakonye, L. A. C., Njoku, J. N., Odirichukwu, J. C., Okolie, S. A., Uzondu, C., … Kim, D.-S. (2023). Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review. Applied Sciences (Basel, Switzerland), 13(3), 1252. doi:10.3390/app13031252

Oman, S. (n.d.). Understanding well-being data: Improving social and cultural policy, practice and research. Nature.

Rajakumaran, G., Venkataraman, N., & Mukkamala, R. R. (2020). Denial of service attack prediction using gradient descent algorithm. SN Computer Science, 1(1). doi:10.1007/s42979-019-0043-7

Ramzan, M., Shoaib, M., Altaf, A., Arshad, S., Iqbal, F., Castilla, Á. K., & Ashraf, I. (2023). Distributed denial of service attack detection in network traffic using deep learning algorithm. Sensors (Basel, Switzerland), 23(20), 8642. doi:10.3390/s23208642

Rusyaidi, M., Jaf, S., & Ibrahim, Z. (2022). Detecting distributed denial of service in network traffic with deep learning. International Journal of Advanced Computer Science and Applications : IJACSA, 13(1). doi:10.14569/ijacsa.2022.0130105

Shi, W.-C., & Sun, H.-M. (2020). DeepBot: a time-based botnet detection with deep learning. Soft Computing, 24(21), 16605–16616. doi:10.1007/s00500-020-04963-z

Shieh, C. S., Nguyen, T. T., & Horng, M. F. (n.d.). Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric. Neural Networks Featuring Geometrical Metric. Mathematics, (9).

Vigneswaran, R. K., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018). Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE.

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying convolutional neural network for network intrusion detection. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE.

Wahab, F., Zhao, Y., Javeed, D., Al-Adhaileh, M. H., Almaaytah, S. A., Khan, W., … Kumar Shah, R. (2022). An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health. Computational Intelligence and Neuroscience, 2022, 6096289. doi:10.1155/2022/6096289

Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. (2021). AE-MLP: A hybrid deep learning approach for DDoS detection and classification. IEEE Access: Practical Innovations, Open Solutions, 9, 146810–146821. doi:10.1109/access.2021.3123791

Yuan, X., He, P., Zhu, Q., & Li, X. (2019). Adversarial examples: Attacks and defenses for deep learning. IEEE Transactions on Neural Networks and Learning Systems, 30(9), 2805–2824. doi:10.1109/TNNLS.2018.2886017

Yuan, X., Li, C., & Li, X. (2017). DeepDefense: Identifying DDoS attack via deep learning. 2017 IEEE International Conference on Smart Computing (SMARTCOMP). IEEE.

Zainudin, A., Kim, D. S., & Lee, J. M. (2022). A Lightweight Deep Learning-based Anomaly Detection and Classification in Software-Defined Industrial Network. In Proceedings of the Korea Communications Society Conference (pp. 1116–1117).

Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2019). Network intrusion detection: Based on deep hierarchical network and original flow data. IEEE Access: Practical Innovations, Open Solutions, 7, 37004–37016. doi:10.1109/access.2019.2905041

DDoS 2019. (n.d.). Retrieved March 25, 2023, from Unb.ca website: https://www.unb.ca/cic/datasets/ddos-2019.html.