*Grenze International Journal of Engineering and Technology, June Issue*

# An Enhanced Real Time DDoS Attack Detection using LSTM and Double DQN with Dueling Networks

Rachana Kamble[1] and Amar Nayak[2]
[1-2]Department of Computer Science and Engineering, Technocrats Institute of Technology (Excellence), Bhopal, M.P., India
Email: rachanakamble@gmail.com, amar.n1975@gmail.com

***Abstract*— The role of Artificial Intelligence, especially deep learning, is important in advanced persistent threats, cyber threat intelligence, mitigate attacks, and to detect malicious cyber activities. New and unseen cyber-attacks such as zero-day attacks, polymorphic malware, and DDoS attacks are not easily detected by traditional machine learning algorithms. Deep learning algorithms such as Long Short-Term Memory and Deep Q-Network can be very efficient for improving DDoS attack detection, cyber security mechanisms, and reliability in information transmission. The proposed model combines DQN with LSTM, Double DQN (DDQN), and Dueling Networks to improve DDoS attack detection. LSTM captures temporal DDoS traffic patterns and inputs its hidden state to the DDQN for decision-making. Double DQN separates the evaluation processes and action selection for more stable learning and to overcome the overestimation bias in DDQN Q-value updates. Dueling DQN divided the Q-value into value functions for specific states and advantage functions for comparing states to other states. Dueling DQN and Double DQN makes the DDoS detection system more robust when making decisions under rapidly changing network conditions and in real-time and also improves the reliability of the learning process. The proposed model is evaluated using evaluation metrics such as F1 score, recall, precision, and accuracy and measures its real-time performance in terms of response times and latency. The experimental outcome indicates that the proposed models' accuracy is 98.81%, precision is 98.91%, recall is 99.02%, and F1-score is 98.89%, which is improved as compared to the Ensemble CNN, RNN, and LSTM model.**

***Keywords*— DDoS, Machine learning, Deep learning, LSTM, DQN, Dueling network, Cyber security.**

## I. INTRODUCTION

According to a Kaspersky report, DDOS attacks are expected to increase by over 400% in 2026. In recent years, cybersecurity has seen significant advances in computer systems discipline and focus on protection of sensitive information that can be obtained to corrupt, damage, and destroy. In the current scenario, Distributed Denial-of-Service attacks are the biggest threat [1]. In DDoS attacks, the central server is bombarded with simultaneous data requests, which may be from multiple compromised systems [2]. The purpose of DDoS attack is to exhaust the target's RAM and Internet bandwidth to disrupt its business and crash the target's system. Sometimes it is very difficult to identify DDos attack because it blocks the identity of the actual source. In these attacks, VPN, websites, and VoIP services are compromised by different intruders and overfill multiple requests to the victim's machine by using botnets; due to that, they deny or sometimes fail to manage the illegal requests. Anomaly-based techniques ensure accurate threat detection and security in network [3].

*Grenze ID: 01.GIJET.12.2.544*

Artificial intelligence is useful for developing cybersecurity approaches to support cyberattack predictions [4], preservations of various privacy approaches [5], examinations based on forensic [6], also for the discovery of several malware's [7]. Traditional machine learning techniques provide solutions to many DDoS attacks, but there are still several limitations in terms of accuracy and performance. There are various limitations of traditional machine learning algorithms, like ethical concern, deterministic problems, lack of data, lack of interpretability, and lack of reproductivity[8].

As deep learning is a subpart of machine learning, both techniques are very useful for implementing neuron, such as math- ematical calculations for solving tedious tasks [9]. A DL threat-enabled detection scheme used a combination of techniques such as DNN (Deep Neural Network) and LSTM (Long Short-Term Memory) for multicast detection of malware families in IoT-based infrastructure [10]. This compound technique is very useful and provides higher detection accuracy for IoT threats. For reliable detection, various supervised and unsupervised techniques are discovered here for perfect malware detection. In DL (Deep Learning), neuron structures are used for learning methods. That is very essential for various areas like computer vision, NL processing, speech processing, and many more. Deep learning factors with hybrid technologies like convolutional neural networks, auto-encoders, and current neural network approaches are useful for investigating anomaly-based intrusion detection techniques[11].

Sometimes AI with DL for cyberattack detection fails due to lack of coloration and high-tech malware design technique[12]. Deep learning methods such as RNN, CNN, reinforcement learning, and LSTM are the most suited methods to detect DDoS attacks on networks and can perform complex tasks and make decisions based on deep analysis[13]. DNN and CNN approaches are very helpful for detecting new malware and different DDoS attacks. Reinforcement learning techniques can be applied to adaptively respond to changing DDoS attack patterns. The limitations of DQN are sample inefficiency, handling continuous action spaces, instability, temporal pattern recognition, and imbalances of data handling that can be overcome by DDQN with dueling.

The proposed DDoS detection system uses a combination of LSTM and (DDQNs) with dueling networks. The goal of our proposed model is to create an efficient and adaptive detection system for DDoS attacks and identify abnormal traffic patterns, and make real-time decisions to mitigate DDoS attacks.

The proposed method used LSTM, Double DQN with Dueling Networks for accurate and stable decision-making. The main contributions are summarized as follows.

- The proposed method combines LSTM and Double DQN with Dueling Networks to enhance the adaptability, efficiency, and accuracy of the detection system.
- The proposed method pre-trains the LSTM model for traffic classification, then fine-tunes it using Dueling DQN and Double DQN, making the DDoS detection system more robust when making decisions under rapidly changing network conditions and real time and also improving the reliability of the learning process.
- The enhanced DQN reward function balances the trade-off between avoiding false positives and detecting attacks.
- The proposed model is evaluated using evaluation metrics such as F1 score, recall, precision, accuracy, and measuring its real-time performance in terms of response times and decision latency.

The paper is organized as follows: Section II represents related work of DDOS attacks using machine learning and deep learning. Section III provides a proposed system model, system architecture, and algorithm for DDoS attack detection. Section IV represents implementation and result analysis. Section V provides a conclusion and future work.

## II. Related Work

Yin et al. [14] proposed an SDN-IoT framework for detecting and mitigating DDoS attacks. The framework consists of an IoT gateway, SD-IoT controllers, SD-IoT switches, and IoT devices. The algorithm uses packet-in message rate with cosine similarity of the vectors at boundary SD-IoT switch ports to identify occurrence of DDoS attacks in SDN-IoT. The frameworks performance and adaptation in the SDN-IoT network to strengthen the security of the IoT with vulnerable and heterogeneous devices are represented by experimental results. According to Fouladi et al. [15], it has worked on a convolutional neural network, which is very helpful to detect DDoS attacks occurring on SDN as it knows deep learning approaches, which are a lot of expensive on undergoing networks. It's convenient to use continuous wavelet transform (CWT) for feature extraction. Elsayed et al.[16] anticipated DDoSNet, according to that in software defined network (SDN) used CICDDoS2019 dataset for detection of DDoS attacks. A recurrent neural network (RNN) is used by DDosNet that is dedicated to sequential data. The RNN has a correspondence with an ANN (Artificial Neural Network) and an autoencoder

that is useful for input to encode and decode noise reduction and anomaly detection. This research work provides accuracy of 99% for DDosNet and 98.8% for AUC and also provides classical machine learning models.
Chen et al. [17] anticipated a prototype for finding DDoS attacks. This research implemented various prototypes like multi- channel convolutional neural network (MCNN), unique preprocessing, DADMCNN, and incremental training. This concept takes input from MCNN and also involves traffic features, host features, and packet features. This work also adds a new convo- lution layer for an effective, appropriate model. Higher accuracy is calculated by various machine and deep learning prototypes like RF, SVM, CNN, LSTM, and KNN.
Ismail et al. [18] proposed a prediction and classification approach for DDoS attack detection using machine learning based on XGBoost and Random Forest algorithms. The model is tested on the UNWS-np-15 dataset, and performance is measured using confusion matrix, precision, accuracy, and F-score.
Tas et al. [19] propose a novel SIP-based attack (SR-DRDoS) that exploits SIP features by using DDoS attack logic, reflection-based attack logic, and IP-spoofing techniques. The attack, when initiated, increased the SIP server CPU load from 0%-100% within 4 minutes. The author also developed a DRDoS attack defense mechanism that reduces the SIP server CPU load to its normal work within 3 minutes. Civitc et al.[20] proposed logistic model trees boosting method DDoS traffic de- tection in IoT network. The framework generates different models for different classes of devices. The framework categorized device classes as Class 1—very high, Class 2—high, Class 3—medium, and Class 4—low traffic predictability. The accuracy of the technique is between 99.93% and 99.98%, indicating the effectiveness of DDoS traffic detection and device classifica- tion.
Liu et al.[21] represent an improved Mirai botnet that makes the edge LR-DDoS attack more obfuscate and powerful in their activity. The author developed an innovative hybrid intrusion defense and detection for LR-DDoS attacks in edge environ- ments. The method employed is Deep Convolution Neural Network (DCNN) and locality-sensitive feature extraction with deep reinforcement learning Q-network for decision-making to defend from LR-DDoS attacks.

## III. Proposed Technique

In this section, system architecture, and a proposed algorithm are provided. This paper proposes enhanced real-time DDoS attack detection using LSTM and Double DQN with Dueling Networks.

### *A. System Architecture*

System architecture consists of data sets, an LSTM model for feature extraction, and double DQN with Dueling Networks for decision-making. This novel combination of LSTM and DDQN with dueling networks allows the system to select the best feature, leading to better evolving and distributed DDoS attack detection accuracy. Fig. 1 represents the system architecture of the proposed work. The hybrid LSTM and DDQN with dueling networks model removes the limitations of DQN, making the DDoS detection model more adaptive, efficient, and robust. The proposed hybrid model provides strong DDoS detection mechanisms by offering faster training, better detection of evolving attack patterns, and improved real-time performance.

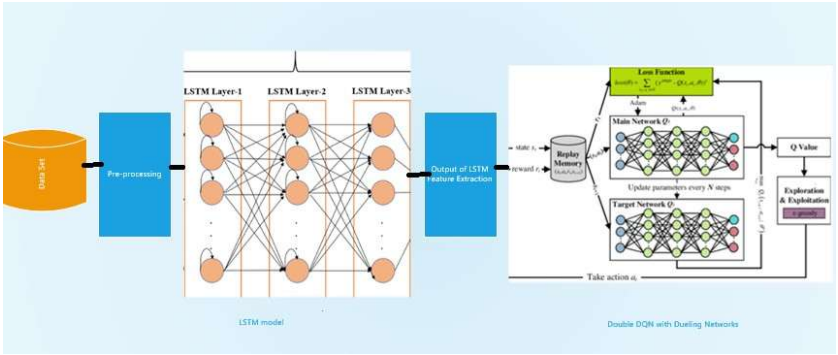


Fig. 1: System Architecture

The proposed architecture integrates LSTM networks for useful feature extraction from data sets and a Double DQN with Dueling Networks. This proposed hybrid architecture will provide efficient and stable detection of DDoS attacks. The data sets such as CIC-DDoS2019, NSL-KDD, or CAIDA can be used as input to the LSTM model. The data preprocessing step is performed to clean the data, normalize it, and extract relevant features such as source IP, duration, and packet size before input to the LSTM model. LSTM network input features may

consist of traffic volume per protocol (ICMP, UDP, TCP), number of connections per second packet inter-arrival time, packet flow duration, source and destination IP addresses, packet size, etc. The output of the LSTM model is input to DDQN with a dueling network. Integration of Dueling Network can effectively determine which actions are valuable and which states are advantageous. It separates Q-value into value and advantage streams. It increases decision- making and accuracy when the state value is low or high. Experience replay is used to store buffers with past experiences. Based on the Double DQN output $\varepsilon -$ greedy policy used to select an action for the next state.

*B. Proposed Algorithm*

The objective of the proposed method is to improve existing DDoS attack detection mechanisms by analyzing and design- ing intelligent DDoS attack detection mechanisms to increase the accuracy of DDoS attack detection with a decrease in false alarms and improve the performance of the network with high security. By drawing on insights from intelligence DDoS attack- detection mechanisms, LSTM, DDQN with dueling networks and reducing false alarms in DDoS detection, it is possible to design an efficient deep learning model for improving DDoS detection, cyber security mechanisms, and reliability in informa- tion transmission.

The proposed algorithm "DDoS Attack Detection using LSTM and Double DQN with Dueling Networks" is represented below. The proposed algorithm provides an efficient and adaptive DDoS attack detection system. The hybrid LSTM, DDQN, and du- eling network algorithm identified abnormal traffic patterns to mitigate DDoS attacks to make real-time decisions. Since DDoS attacks evolve over time, the model needs to understand the temporal sequence of network traffic data. LSTM can efficiently understand the temporal sequence of network traffic data as it can capture patterns in sequential data and model long-term de- pendencies.

The inputs to the algorithm are the network traffic data stream, LSTM parameters, primary DQN network, target DQN network, replay buffer, reward function, discount factor, learning rate, and exploration rate. The output of the algorithm is an optimal action, which may flag, allow, or block the traffic. In the first step, we initialize all the parameters, such as learning rate, replay buffer, exploration rate, and discount factor, with some initial values. It also initializes LSTM parameters, target network, and DDQN network. The next step is temporal network traffic data collection and fetaure normalization for LSTM input. In the action selection step, the algorithm can choose a random action with probability as exploration or exploitation as the highest Q-value selection action. Next execute action will perform where traffic can be flagged, allowed, or blocked according to action selected by the network. The reward is observed based on action correctness. The next hidden state can be computed from traffic data and set the current state as a hidden state. The experience is stored in replay buffer. The next step is to create a mini batch sample from the replay buffer and compute the target value computation using the target network. The primary network updation is performed by minimizing the loss. If the network finds a loss, then perform a gradient descent operation to optimize the loss. The input to the LSTM network is temporal traffic features. The LSTM encodes temporal dependencies in the traffic flow af- ter processing sequential data and outputs a hidden state. This hidden state is input to the DDQN with dueling networks for decision-making.

Dueling DQN divided the Q-value into a value function for a specific state and an advantage function for comparing the state to other states. Dueling DQN and Double DQN makes the DDoS detection system more robust when making decisions under rapidly changing network conditions and real time and also improves the reliability of the learning process. The target network is periodically updated with the primary network. The DDQN is trained by random sampling of mini-batches and getting ex- periences stored in a buffer from environment interacting. The model can learn efficiently without correlations of consecutive samples. To mitigate the overestimation bias in Q-learning, the Double DQN algorithm is used, and to ensure stable learning, the target network is periodically updated.

DDoS detection algorithm used LSTM and Double DQN with Dueling Networks uses CIC-DDoS2019 and CIC-DDoS2017 datasets for evaluating and training the model.

TABLE I: HARDWARE AND SOFTWARE CONFIGURATIONS

| | |
|---|---|
| Manufacturer | HP |
| Processor | Intel Core Ultra 9 (Series 2) with 4.8GHz |
| GPU | NVIDIA GetForce RTX |
| Memory | 16 GB |
| Operating system | Windows 11 |
| Deep learning framework | Keras and TensorFlow |
| Development framework | Anaconda and Jupyter notebook |
| Python version | 3.11 |

Algorithm 1 DDoS Attack Detection using LSTM and Double DQN with Dueling Networks

1: Input: Network traffic data stream $X$, LSTM parameters, primary DQN network $Q(s, a; \theta)$, target DQN network $Q'(s, a; \theta')$, replay buffer $D$, reward function $r$, discount factor $\gamma$, learning rate $\alpha$, exploration rate $\varepsilon$
2: Output: Optimal action $a \in$ {Block, Allow, Flag}
3: Initialize replay buffer $D$
4: Initialize LSTM network parameters
5: Initialize primary DQN $Q(s, a; \theta)$ and target DQN $Q'(s, a; \theta')$ 6: Set exploration rate $\varepsilon$, learning rate $\alpha$, and discount factor $\gamma$ 7: for each episode (or incoming traffic sequence $X$) do
8: Traffic data pre-process $X$: $X = \{x_1, x_2, \ldots, x_T\}$
9: Features standardization or normalization or features
10: Pass pre-processed traffic data $X$ through LSTM to find $h_T$: $h_T = \text{LSTM}(X)$ 11: Set state as $s_T = h_T$
12: *// Selection of action using ε-greedy policy*
13: if random_probability $< \varepsilon$ then
14: Random action Selection as $a_T$ (exploration) 15: else
16: Action Selection $a_T = \text{argmax}_a Q(s_T, a; \theta)$ (exploitation) 17: end if
18: Action Execution $a_T$ (Block, Allow, Flag)
19: Reward Observation $r_T$ and next sequence of traffic
20: Passing of next traffic sequence through LSTM to get the value of $h_{T+1}$: $h_{T+1} = \text{LSTM}(X_{\text{next}})$ 21: Next state setting $s_{T+1} = h_{T+1}$
22: $D$ the replay buffer stores experience as $(s_T, a_T, r_T, s_{T+1})$. 23: *// Experience Replay and Training*
24: if replay buffer $D$ has enough samples then
25: Sample mini-batch $\{(s_i, a_i, r_i, s_{i+1})\}^N$ from $D$
26: for each sample $i$ do
27: Compute target $y_i = r_i + \gamma Q'(s_{i+1}, \text{argmax}_a Q(s_{i+1}, a; \theta); \theta')$ 28: Update primary DQN by minimizing loss:
29: $L(\theta) = \frac{1}{} \sum_i (y_i - Q(s_i, a_i; \theta))^2$
30: Perform gradient descent to update $\theta$ 31: end for
32: end if
33: *// Periodic target network update* 34: if target update condition met then 35: Update target network: $\theta' \leftarrow \theta$ 36: end if
37: end for

## IV. Simulation Configuration, Dateset, and Simulation Result, Performance Analysis

This section briefly represents the proposed model experimental setup, dataset description, and discusses the classification re- sults. Results analysis is performed based upon the f-measure, detection accuracy, recall, precision, training, and testing duration. The implementation is performed on i5 3.50GHz Intel CPU computer system with 16GB of RAM and the Windows 11 oper- ating system. Python programming language, Anaconda framework, Jupyter notebook, and TensorFlow are used to implement the proposed model.

*System hardware and software specifications*

The table II represents the hardware and software configuration used in implementation of proposed model. It provides details of processor, RAM, Python and Jupyter notebook.

Table II: Parameters used

| Parameter | Description | Value |
|---|---|---|
| Hidden layers | Number of LSTM hidden layers | 6 |
| Epoch | Number of epoch | 100-300 |
| Optimizer | Gradient descent | 0.1-0.3 |
| Biases | Model biases | Random |
| Learning rate | model learning | 0.003-0.006 |

Table III: Datasets description

| Datasets | Events/ Attacks | Testing events (flows) | Training events (flows) |
|---|---|---|---|
| CICDDoS 2019 | DrDNS | 1(4902) | 1(22982) |
| | SYN | 1(989944) | 1(886817) |
| | Benign | 1(41853) | 1(92720) |

| | | | |
|---|---|---|---|
| | UDP | 2(1022869) | 1(989247) |
| | Total Flows | 2059568(51%) | 1991766(49%) |
| CICDDoS 2017 | DoS GET | 1(766) | 3(2304) |
| | DDoS GET | 1(5015) | 1(5497) |
| | Slow-send body | 2(1002) | 6(3025) |
| | Benign | 1(42473) | 1(83075) |
| | Slow-read | 1(2133) | 1(2133) |
| | Improved GET | 1(532) | 2(1222) |
| | Slow-send header | 3(3952) | 4(5436) |
| | Total Flows | 55873(35%) | 102692(65%) |

*List of parameters*

Table III represents the list of parameters used in the implementation of the proposed algorithm. Datasets description:

The most widely used datasets for DDoS attacks are CIC-DDoS2019 [? ], CAIDA 2007, NSL-KDD, CSE-CIC-IDS2018, TON_IoT Datasets, and LOIC DDoS Dataset. CICDDoS2019 contains the most up-to-date common DDoS attacks in PCAP format. It also includes the CICFlowMeter-V3 network traffic analysis tool, labeled flows-based data on attacks and protocols, destination and source ports, destination and source IPs, and a time stamp in CSV format.

Datasets statistics Table IV represents the database statistics of the CICDDoS 2017 and CICDDoS 2019 datasets. The CICDoS- 2017 dataset contains six different attacks and 26 attack events, out of which we used nine events for testing and 17 events for model training. CICDDoS2019 dataset generated from three capturing days of the attacks for testing and training. We consider DoS GET, Benign, Slow-read, Improved GET, DDoS GET, Slow-send header, and Slow-send body attacks events from testing data 35% and training data 65% from CICDDoS 2017 and SYN, UDP number, Benign, and Dr.DNS of flows testing events 51% and 49% training events.

*A. Performance Analysis*

This section represents a performance analysis of the proposed method. Accuracy: is correct classification proportion (true neg- atives and true positives) from overall number of cases. Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$

Recall: Proportion of correct positive classifications (true positives) from cases that are actually positive.

$$Recall = \frac{TP}{TP+FN}$$

Precision: Proportion of correct positive classification (true positives) from predicted as positive cases.

$$Precision = \frac{TP}{TP+FP}$$

F- Score or F-Measure, is a single measure of classification procedure usefulness. To compute the score F-Score considers both precision and recall of the cases. The lowest possible F-Score is 0. $0 \leq F \leq 1$

Harmonic mean of precision and recall is the F-Score. $F = \frac{2}{\frac{1}{recall} + \frac{1}{Precision}}$

$$F = 2 * \frac{precision * recall}{precision + recall}$$

Confusion matrix A confusion matrix is performed by the classification system to represent the information related to the actual and predicted classifications.

The proposed method CPU utilization is 6.01%, Ensemble CNN is 6.03, Ensemble RNN is 15.99, and BLSTM is 13.82. It represents our technique performance in DDoS attack detection. Confusion matrix: Ensemble LSTM The figure 3 represents precision, recall, F1-score, and DM of the proposed technique, Ensemble CNN, Ensemble RNN, and Ensemble ELSTM. The accuracy of the proposed techniques, Ensemble CNN, RNN, and BLSTM, is 98.81, 98.77, 83.28, and 86.28, respectively. It represents that the accuracy of the proposed technique is improved as compared to other techniques. The precision of the proposed techniques, Ensemble CNN, RNN, and BLSTM, is 98.91, 98.87, 96.1, and 88.22, respectively. The recall of the proposed technique is 99.02, Ensemble CNN is 98.88, RNN is 73, and BLSTM is 98.02. The F1-score of the proposed technique is 98.89, Ensemble CNN is 98.76, RNN is 83.84, and BLSTM is 93.46. It represents that the proposed technique is efficient to detect DDoS attacks in networks. The DDoS detection ration is also improved to 99.15 in the proposed technique. The confusion matrices of proposed Ensemble CNN, Ensemble RNN, and BLSTM are presented in Figures , 5, 6, and 7, respectively. Predicted label and true label represent the description of

predicted and actual classes. Confusion matrix parameters represent the complete performance descriptor and help in determining model evaluation metrics. The accuracy is confirmed using diagonal values represented in the confusion matrix number of samples. The figure 7 represents the testing time of different DDoS detection techniques in minutes. The testing time of the proposed technique is 0.061, and Ensemble CNN is 0.062.
Figure 8 provides training time for different DDoS attack detection techniques in minutes. The training time of the proposed technique is 35.22, Ensemble CNN is 38.22, Ensemble RNN is 91.96, and BLSTM is 47.00. The reduction in training time represents the effectiveness of our method. The figure 9 provides the CPU utilization of different DDoS attack detections.

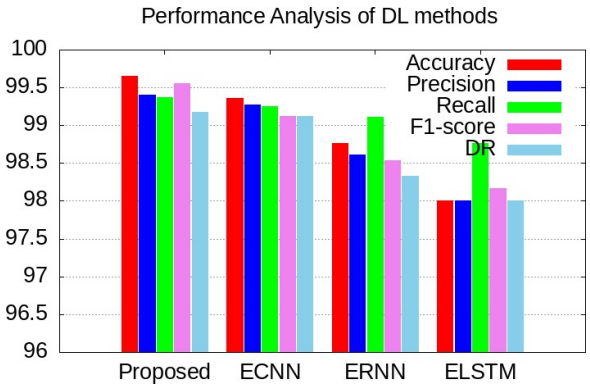


Figure. 2 Precision, Recall, F1-score, DM

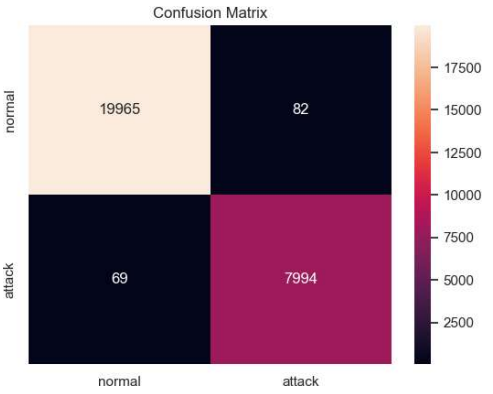


Figure 3. Confusion Matrix: Proposed Method

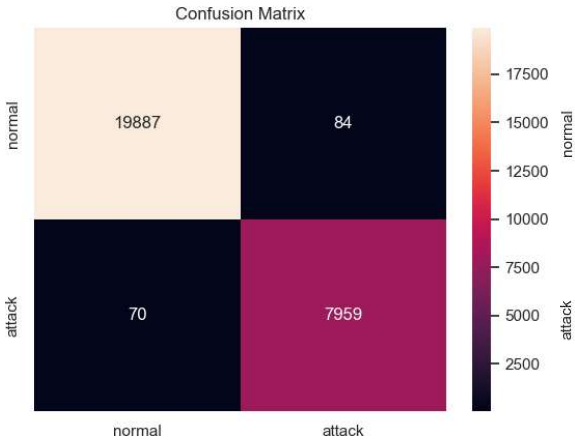


Figure 4. Confusion Matrix: Ensemble CNN

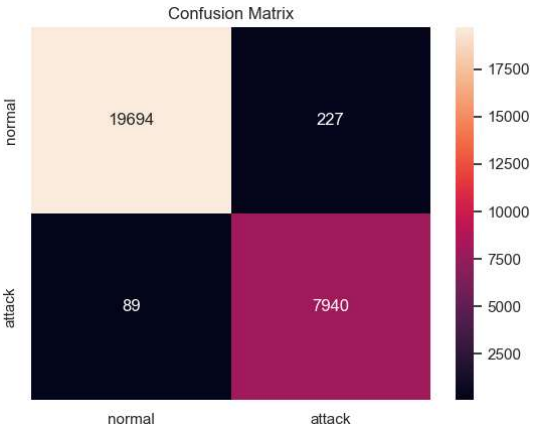


Figure 5. Confusion Matrix: Proposed Method

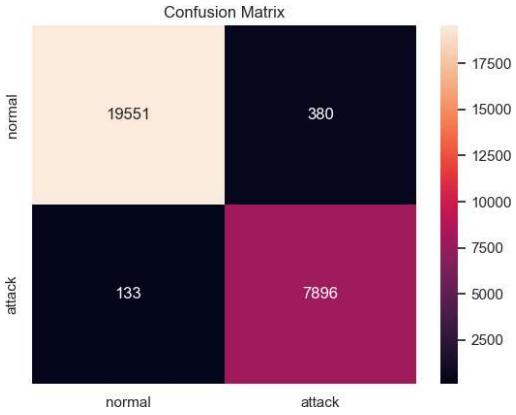


Figure 6. Confusion Matrix: Ensemble RNN

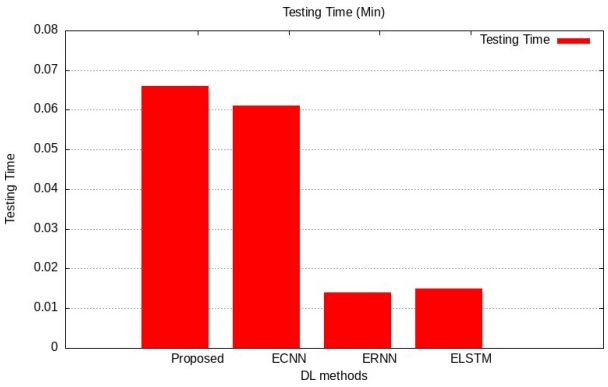


Figure7. Confusion Matrix: Ensemble RNN

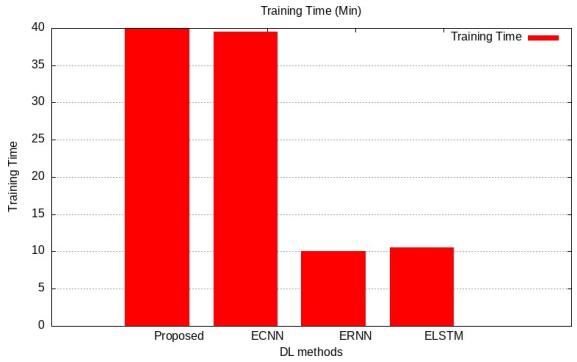


Figure 8. Confusion Matrix: Ensemble RNN

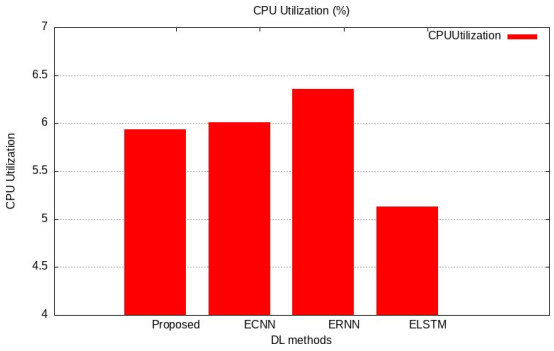


Figure 7. Confusion Matrix: Ensemble RNN

TABLE IV: COMPARISON OF PROPOSED METHOD WITH OTHER DL METHODS

| Method | Accuracy | Precision | Recall | F1 | Test time | Train time | CPU usage |
|---|---|---|---|---|---|---|---|
| Proposed | 98.81 | 98.91 | 99.02 | 98.89 | 0.061 | 35.22 | 6.01 |
| Ensemble CNN | 98.77 | 98.87 | 98.88 | 98.76 | 0.062 | 38.22 | 6.03 |
| RNN | 83.28 | 96.1 | 73 | 83.84 | N/A | 91.96 | N/A |
| BLSTM | 86.28 | 88.2 | 98.2 | 93.46 | N/A | 4700 | N/A |

## V. CONCLUSION

AI techniques such as deep learning can be trained to automatically scan for unknown malware rather than specific signatures, zero-day exploitation based on certain features and behaviors. The proposed hybrid model integrates LSTM networks for feature extraction and a double DQN with dueling networks for decision-making and provides efficient, stable detection of DDoS attacks. The designed method provides an intelligent attack detection mechanism using LSTM and DQN in the field of cyber security with high detection accuracy. The proposed model successfully detects and classifies DDoS attacks to prevent networks from crashing. The proposed model is evaluated using evaluation metrics such as F1 score, recall, precision, and accuracy and measures its performance in terms of decision latency and response times. Experimental outcome indicates that proposed model accuracy is 98.81%, precision is 98.91%, recall is 99.02%, and F1-score is 98.89%, which is improved as compared to Ensemble CNN, RNN, and LSTM models.

## REFERENCES

[1] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the internet of things using hybrid deep learning model," IEEE Access, vol. 11, pp. 119 862– 119 875, (2023)

[2] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," IEEE Access, vol. 6, pp. 48 231–48 246, (2018)

[3] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, "Machine learning in network anomaly detection: A survey," IEEE Access, vol. 9, pp. 152 379–152 396, (2021)

[4] A. Swaminathan, B. Ramakrishnan, K. M, and S. R, "Prediction of cyber-attacks and criminality using machine learning algorithms," in 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), pp. 547–552 (2022)

[5] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial iot networks through a reliable cyberattack detection model," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154–6162, (2020.)

[6] A. M. Qadir and A. Varol, "The role of machine learning in digital forensics," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5 (2020)

[7] S. B. Mane, S. Jadhav, C. Gamre, S. Gharat, J. Patil, and V. Raina, "Cyber-malware detection using machine learning," in 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 915–920, (2023)

[8] M. F. Ashfaq, M. Malik, U. Fatima, and M. K. Shahzad, "Classification of iot based ddos attack using machine learning techniques," in 2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), pp. 1–6 (2022)

[9] Meenakshi, K. Kumar, and S. Behal, "Distributed denial of service attack detection using deep learning approaches," in 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 491–495 (2021)

[10] M. Sinthuja and K. Suthendran, “Ddos attack detection using enhanced long-short term memory with hybrid machine learn- ing algorithms,” in 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), pp. 1213–1218 (2022)
[11] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, “Machine learning for anomaly detection: A systematic review,” IEEE Access, vol. 9, pp. 78 658–78 700 (2021)
[12] P. Singh, S. Kaur, S. Sharma, G. Sharma, S. Vashisht, and V. Kumar, “Malware detection using machine learning,” in 2021 International Conference on Technological Advancements and Innovations (ICTAI), pp. 11–14 (2021)
[13] S. Singh, M. Gupta, and D. K. Sharma, “Ddos attack detection with machine learning: A systematic mapping of literature,” in 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 939–945 (2023)
[14] D. Yin, L. Zhang, and K. Yang, “A ddos attack detection and mitigation with software-defined internet of things framework,” IEEE Access, vol. 6, pp. 24 694–24 705 (2018)
[15] R. F. Fouladi, O. Ermi¸s, and E. Anarim, “A novel approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-defined network,” Computers Security, vol. 112, p. 102524, (2022) [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003485
[16] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, “Ddosnet: A deep-learning model for detecting network attacks,” in 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 391–396 (2020)
[17] K. H. H. J. Z. W. Jinyin Chen, Yi Tang, “Dad-mcnn: Ddos attack detection via multi-channel cnn,” ACM Digital Library, vol. 3, pp. 484– 488, (2019)
[18] Ismail, M. I. Mohmand, H. Hussain, A. A. Khan, U. Ullah, M. Zakarya, A. Ahmed, M. Raza, I. U. Rahman, and M. Haleem, “A machine learning-based classification and prediction technique for ddos attacks,” IEEE Access, vol. 10, pp. 21 443–21 454 (2022)
[19] I. M. Tas, B. G. Unsalver, and S. Baktir, “A novel sip based distributed reflection denial-of-service attack and an effective defense mechanism,” IEEE Access, vol. 8, pp. 112 574–112 584, (2020)
[20] I. Cviti c, D. Perakovic, B. B. Gupta, and K.-K. R. Choo, “Boostingbased ddos detection in internet of things systems,” IEEE Internet of Things Journal, vol. 9, no. 3, pp. 2109–2123 (2022)
[21] Z. Liu, X. Yin, and Y. Hu, “Cpss lr-ddos detection and defense in edge computing utilizing dcnn q-learning,” IEEE Access, vol. 8, pp. 42 120– 42 130 (2020)