International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Deep Learning Based Network Attack Classification

Nagarjuna Reddy.G[1],Dinsh.V[2],Pavan Kumar.K[3], Mrs.Jeeva.V[4], Dr.Kiruba devi[5]

[1,2,3,4,5]Dr.M.G.R Educational and Research Institute, Madhuravoyal, Chennai,India.

Abstract:
The most common security threads to internet service is distributed denial of service also known as DDoS attack. This DDoS can be easily be launched in pc, cloud service providers and many more that suddenly spikes in traffic or websites slowdown. There are traditional DDoS attack detection are present which uses ML based algorithms gives accuracy but if the dataset consists of large volume of data the traditional algorithms find difficult to detect. Since Deep learning is widely used in present days, which is powerful learning and has extraction capabilities. In this paper we used LSTM which is a type of Recurrent Neural Network (RNN) which are Deep Learning based algorithms. In this paper WSN-DS.cv dataset is used, the data set consists of wireless sensor network classifications. Here we train the raw data by preprocessing of data like feature extraction, identifying the null values, analysing the data and splitting them for train and test. Here we epoch the dataset for 10 times to get better accuracy

Keywords: Deep learning, LSTM, RNN, DDoS, CNN, IoT.

1. INTRODUCTION

The DDoS attack is an cyber attack that goes into pc laptops, Iot devices and many more. This DDoS attack a target websites or swervers or network though flooding it with traffic Causing lagging issues, they mainly provide users from accessing websites and servers. The main aim of attack is flood resources like memory, bandwidth, processing capabilities and denay all other access to websites.

The systems which are targeted usually get suffered and these results in duration of longtime, less security, loss of revenue. Some times this DDoS is used for distraction for users so that the hackers can crack the firewall and enter their privacy data, steel imp data, accessing their accounts and many more..

In previous tradition based techniques have widely used to detect the DDoS attack, those methods showed their limits due to lack of adaptability to other new attack patterns

Deep learning play an crucial role for evolving different DDoS attack patterns because traditional methods face challenges in detecting them due to their rapid evolution of attack patterns.

In modern methodology likes random forest, xg boost which I have researched they give best accuracy but it depends upon the type of dataset we are training, for dataset like time series LSTM it is mostly used.9

1.1 TYPES OF DDoS ATTACK

a. IMCP FLOOD

It is an internet control message protocol flood attack, the attack sends a large number o packets and overloading with traffic.

b. SYN FLOOD

It is an synchronization flood attack, the attacker sends large amount of packets and ability to legitimate connection request.

c. UDP FLOOD

It is user datagram protocol sends packets and cause network traffic

d. HTTP FLOOD

Here attacker sends large number of HTTP requests to target web server, overloading it with traffic and preventing users from accessing websites.

2. LITERATURE SURVEY

J. Doe et al.[1] In 2023, researchers proposed deep neural network model for classification in IoT environments. Their study evaluated performance using benchmark datasets such as UNSW-NB15 and CIDDS-001, achieving high accuracy by leveraging optimized hyperparameters.

Smith et al. [2] A 2022 systematic review on hybrid deep learning models for intrusion detection outlined how combining multiple deep learning techniques enhances detection accuracy and efficiency. This study emphasized the strengths of hybrid models in addressing network security threats.

Johnson et al. [3] Researchers in 2023 introduced an approach that integrates network and host data using deep learning for intrusion detection. By analyzing both network traffic and host activities, the system demonstrated improved classification accuracy and reduced false positives.

Lee et al. [4] A 2024 study reviewed various deep learning architectures utilized for intrusion detection, comparing the performance of CNNs, RNNs, and LSTMs. This analysis provided insights into model selection and optimization techniques for enhanced threat detection.

Kim et al., [5] In 2022, an in-depth analysis was conducted on the application of machine learning and deep learning techniques in Software-Defined Networking (SDN) environments. The study discussed security risks associated with SDN and proposed novel solutions for real-time threat detection.

Wang et al., [6] A 2023 survey explored adversarial attacks on deep neural network-based classifiers and evaluated state-of-the-art defense mechanisms. The findings emphasized the need for robust adversarial training and anomaly detection strategies.

Brown et al. [7] A 2020 review addressed backdoor attacks in deep learning based detection systems, categorizing potential and presenting countermeasures to mitigate risks.

Patel et al., [8] In 2024, researchers examined the effectiveness of CNNs, RNNs, and LSTMs for intrusion detection, highlighting the advantages of recurrent models in capturing temporal dependencies within network traffic.

Wilson et al. [9] A 2021 systematic review discussed artificial neural networks (ANNs) in cybersecurity, covering deep belief networks and generative adversarial networks (GANs) for anomaly detection and intrusion prevention.

Green et al., [10] A 2025 study introduced a novel federated learning approach for intrusion detection, enabling collaborative model training while preserving data privacy. This method improved classification accuracy across distributed network environments.

Black et al., [11] In 2023, researchers investigated transformer-based architectures for network attack classification, demonstrating their superiority in handling sequential network traffic data compared to traditional RNN models.

A N H Dhatreesh Sai, B H Tilak, [12] in 2022 Distributed Denial of Service (DDoS) attacks aim to make a server unresponsive by flooding the target server with a large volume of packets (Volume based DDoS attacks)

Brown et al., [13] A 2022 study examined the effectiveness of graph neural networks (GNNs) in intrusion detection, leveraging graph-based representations of network traffic to capture complex attack patterns.

Davis et al., [14] In 2021, researchers proposed an ensemble deep learning approach that combined multiple models such as CNNs, LSTMs, and attention mechanisms to improve classification performance and reduce false positive rates.

N. Thompson et al., [15] A 2023 review analyzed the impact of dataset quality on deep learning-based intrusion detection, emphasizing the importance of data preprocessing, augmentation, and feature engineering for robust model performance.

3. PROBLEM STATEMENT

The problem statement for the DDoS attack classification is there are many models for detection like traditional methods, machine learning models, and deep learning models. We should choose our model depending upon type of dataset we are training. The traditional methods are time taken process and they cannot detect the present days attack patterns due to lack of training, machine learning models can able to detect them and get god accuracy, f1score. While coming to deep learning methods they are useful for large quantity of data and has greater training capability than ML because deep learning comes under subset machine learning. Here we used LSTM training model which is deep learning based algorithm.

4. EXISTING SYSTEM

The existing systems for DDoS attack there are several machine learning techniques like random forest, XG boost and many more and CNN for deep learning. machine learning algorithms might give more accuracy for datasets, but my dataset consists of more network traffic flow and time series based dependences and sequential data so we used LSTM model which can capture hidden patterns than RF model might miss.

In existing system for sequential data handling LSTM is better suited for time series, in feature engineering machine learning models require manual feature selection while deep learning models like LSTM automatically learn the important features, reducing the human effort. While coming to scalability LSTM can adapt more data is available and perform more than ML algorithms in long run.

5. METHODOLOGY

The objective of this paper is to use the LSTM algorithm which is deep learning based model and find the accuracy and loss of this model for this we used WSN-DS data set for this research from kaggle website.

The architecture consists of data collection which has to be collected from kaggle, preprocessing the data, LSTM algorithm training, model testing and finding the accuracy.

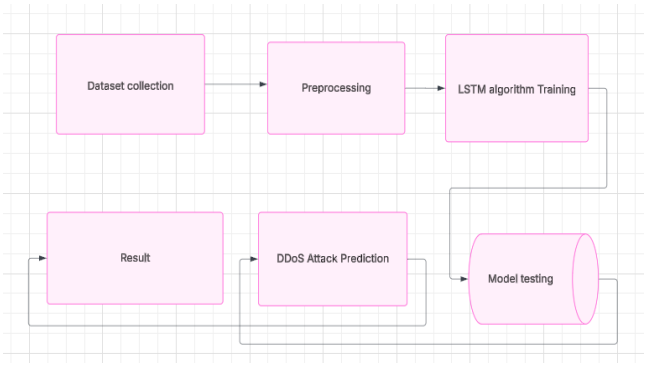

Fig.1 Architecture

This **Fig.1** This architecture diagram shows the pipeline of this process.

5.1 LSTM algorithm

The LSTM stands for long short term memory and it is a type of recurrent neural network RNN which is used for processing the sequential data. In the traditional RNN the information is passed through one step to another unit of network called hidden state. The problem is the RNN suffer from vanishing gradient.
The LSTM architecture corrects the issue by introducing complex unit of memory cell which is able to store and forget information. This cell contains series of gates which control the flow of information into and out of the cell. Overall the LSTM algorithm is powerful tool for processing sequential data and widely used in other applications like natural language processing, speech recognition and time series analysis.

5.2 Dataset Collection

For this paper we used the dataset of WSN-DS which is wireless sensor network, which consists of several patterns and network traffic.

5.3 pre-processing of data

Here the data should be pre processed in terms of Data cleaning which is used to remove the un used data , remove the noise, normalize the features and convert categorial variables to numerical ones.

5.4 feature Extraction

Extract the features from pre-processed data that are used to train LSTM model. They should be packet size, packet duration.

5.5 training of data

Train the LSTM model using the exrtracted features from pre processed data.the LSTM model can be trained using supervised learning approach, where labeled data is used to train model to predict if an incoming traffic is under attack or no.

5.6 Testing of data

Test the trained LSTM model on a separate set of test data to understand its performance in detecting and classifying DDoS attack.
formulas
a.for Accuracy=Total of correct predictions / total number of predictions
b.for Model loss is –[ylog(y^)+(1-y)log(1-y^)]
Where y=actual label from 0 to 1
Y^ is predicted probability between 0 and 1
c.For **MinMaxScaler()** function X-Xmin / Xmax-Xmin
This function ensures that all the variables are normalized between 0 and 1 used in pre processing of data.

5. RESULT AND DISCUSSION

	id	Time	Is_CH	who CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_cod
0	101000	50	1	101000	0.00000	1	0	0	25	1	0	0	0	1200	48	130.08535	
1	101001	50	0	101044	75.32345	0	4	1	0	0	1	2	38	0	0	0.00000	
2	101002	50	0	101010	46.95453	0	4	1	0	0	1	19	41	0	0	0.00000	
3	101003	50	0	101044	64.85231	0	4	1	0	0	1	16	38	0	0	0.00000	
4	101004	50	0	101010	4.83341	0	4	1	0	0	1	25	41	0	0	0.00000	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
374656	201096	1003	0	201051	6.98337	0	5	1	0	0	1	7	96	0	67	170.14779	
374657	201097	1003	0	201037	29.32867	0	5	1	0	0	1	31	39	0	24	82.21043	
374658	201098	1003	0	201095	18.51963	0	5	1	0	0	1	17	55	0	31	139.26438	
374659	201099	1003	0	201051	8.55001	0	5	1	0	0	1	3	96	0	65	158.27492	
374660	202041	1025	0	202100	0.00000	0	5	0	0	0	0	4	7	689	7	115.00407	

374661 rows × 19 columns

Fig.2 dataset

This **Fig.2** contains the dataset information which i was using since it is an WSN data set it contains id, time stamp, cluster head, distance from node, number of advertisement packets, number of data packets and others.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 374661 entries, 0 to 374660
Data columns (total 19 columns):
 #   Column             Non-Null Count   Dtype
---  ------             --------------   -----
 0    id                374661 non-null  int64
 1    Time              374661 non-null  int64
 2    Is_CH             374661 non-null  int64
 3    who CH            374661 non-null  int64
 4    Dist_To_CH        374661 non-null  float64
 5    ADV_S             374661 non-null  int64
 6    ADV_R             374661 non-null  int64
 7    JOIN_S            374661 non-null  int64
 8    JOIN_R            374661 non-null  int64
 9    SCH_S             374661 non-null  int64
 10   SCH_R             374661 non-null  int64
 11  Rank               374661 non-null  int64
 12   DATA_S            374661 non-null  int64
 13   DATA_R            374661 non-null  int64
 14   Data_Sent_To_BS   374661 non-null  int64
 15   dist_CH_To_BS     374661 non-null  float64
 16   send_code         374661 non-null  int64
 17  Expaned Energy     374661 non-null  float64
 18  label              374661 non-null  object
```

Fig.3 feature selection

This **Fig.3** contains of data information in which dataset should contains of all non null values and should be data types, in this image there is an object named label which is not any data type so we have to change it into integer by pre processing of data.

After pre processing and feature selection of data we have to train the data by splitting process as

split = int(0.8 * len(X)) X_train,

X_test = X[: split], X[split :]

y_train, y_test = y[: split], y[split :]

here data is split into 80% for training and 20% for testing.

```
Epoch 1/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 113s 14ms/step - accuracy: 0.9419 - loss: 0.2500 - val_accuracy: 0.9501 - val_loss: 0.1896
Epoch 2/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 107s 14ms/step - accuracy: 0.9518 - loss: 0.1945 - val_accuracy: 0.9608 - val_loss: 0.1574
Epoch 3/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 100s 13ms/step - accuracy: 0.9530 - loss: 0.1881 - val_accuracy: 0.9609 - val_loss: 0.1562
Epoch 4/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 101s 13ms/step - accuracy: 0.9525 - loss: 0.1886 - val_accuracy: 0.9614 - val_loss: 0.1528
Epoch 5/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 108s 14ms/step - accuracy: 0.9526 - loss: 0.1854 - val_accuracy: 0.9606 - val_loss: 0.1544
Epoch 6/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 106s 14ms/step - accuracy: 0.9525 - loss: 0.1859 - val_accuracy: 0.9614 - val_loss: 0.1534
Epoch 7/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 99s 13ms/step - accuracy: 0.9528 - loss: 0.1839 - val_accuracy: 0.9609 - val_loss: 0.1550
Epoch 8/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 141s 13ms/step - accuracy: 0.9536 - loss: 0.1818 - val_accuracy: 0.9616 - val_loss: 0.1542
Epoch 9/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 69s 9ms/step - accuracy: 0.9543 - loss: 0.1795 - val_accuracy: 0.9614 - val_loss: 0.1536
Epoch 10/10
7493/7493 ━━━━━━━━━━━━━━━━━━━━ 107s 14ms/step - accuracy: 0.9532 - loss: 0.1816 - val_accuracy: 0.9614 - val_loss: 0.1528
```

Fig.4 training

This **fig.4** explains the training of dataset through epoch, where epoch is an approach which complete pass through entire training dataset during training.

Here we have done 10 approaches to calculate the accuracy and loss and the model is working properly. The more epochs helps to get better accuracy.

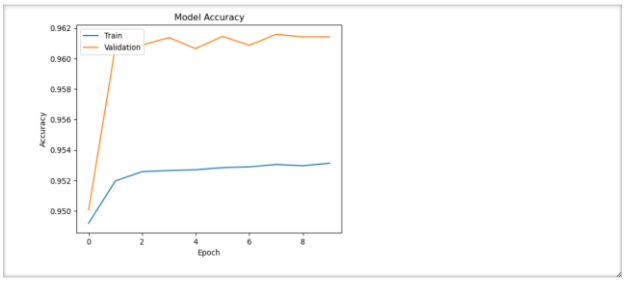

Fig.5 accuracy

This **fig.5** explains the model training accuracy and validation accuracy change over epochs.
Here X-axis epochs is one full pass through training data.
And y-axis is accuracy which gives higher accuracy and its making fewer classifications errors.

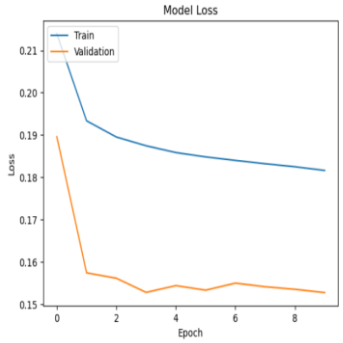

Fig.6 model loss

This fig.6 explains model loss change over the training epochs for both training and validation set, which means decreasing training loss is improving its fit on training set epoch. Decrease in validation loss is also improving on unseen data it suggests no immediate overfitting of dataset for training.
Overall this plot indicates the model is learning effectively and generalizing.

6. CONCLUSION

In this paper we proposed deep learning based DDoS detection using LSTM algorithm which gives us an accuracy of 0.9594 and loss of 0.1634, the accuracy can be increased to its maximum depending upon the dataset we are using since 95% is also an best accuracy and can be included.on this project we found that the structure and quality of data used to train the model plays an important role in their performance obtained. For future work, the LSTM algorithm has shown its results good, the algorithm is able to adapt to new patterns. We need to use more models and algorithms to get better accuracy overall the accuracy depends upon data we are training, LSTM is an valuable tool for detection and should be considered as an part of security strategy for networks.

REFERENCE

1. T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures", International Journal for Information Security Research (IJISR), vol. 5, no. 4,December2015,https://doi.org/10.1109/ICITST.2015.7412116.
2. O. Bello and S. Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things," in IEEE Systems Journal, vol. 10, no. 3, pp. 1172-1182, Sept. 2016, https://doi.org/10.1109/JSYST.2014.2298837.
3. M. Miettinen and A. Sadeghi, "Keynote: Internet of Things or Threats? On Building Trust in IoT," 2018 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Turin, pp. 1-9, 2018, doi: 10.1109/CODESISSS.2018.8525931.
4. M. Abomhara and G. M. Kien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," in Journal of Cyber Security and Mobility, vol. 4, no 1, pp. 65-88, Jan 2015, https://doi.org/10.13052/jcsm2245-1439.414.
5. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 23472376,Fourthquarter2015,https://doi.org/10.1109/COMST.2015.2444095.
6. "The first DDoS attack was 20 years ago," Emerging Technology from the arXiv. [Online]. Available: https://www.technologyreview.com/s/613331/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since/
7. X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, pp. 1-8, 2017,
8. GUPTA, Brij B. et DAHIYA, Amrita. Distributed De-nial of Service (DDoS) Attacks: Classification, Attacks,Challenges and Countermeasures. CRC press, 2021.
9. FENIL, Edwin et MOHAN KUMAR, P. Survey onDDoS defense mechanisms. Concurrency and Compu-tation: Practice and Experience, 2020, vol. 32, no 4, p.e5114.
10. SINGH, Rajeev et SHARMA, T. P. Present Status of Distributed Denial of service (DDoS) attacks in inter-net world. International Journal of Mathematical, Engi-neering and Management Sciences, 2019, vol. 4, no 4, p.1008.
11. SNEHI, Manish et BHANDARI, Abhinav. Vulnerabilityretrospection of security solutions for software-definedCyber–Physical System against DDoS and IoT-DDoS attacks.Computer Science Review, 2021, vol. 40, p.100371.
12. DI MAURO, Mario, GALATRO, Giovanni, FORTINO,Giancarlo,et al. Supervised feature selection techniquesin network intrusion detection: A critical review. Engi-neering Applications of Artificial Intelligence, 2021, vol.101, p. 104216
13. Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," in IEEE Access, vol. 6, pp. 3536535381,2018,https://doi.org/10.1109/ACCESS.2018.2836950.
14. Y. Imamverdiyev and F. Abdullayeva, "Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine," Big Data, vol. 6, no.2,pp.159-169,2018,https://doi.org/10.1089/big.2018.0023.
15. Y. LeCun, Y. Bengio, and G. Hinton, Deep learning.Nature521,436,2015,https://doi.org/10.1038/nature14539.

16. A. S. Unal and M. Hacibeyoglu, “Detection of DDOS Attacks in Network Traffic Using Deep Learning,” International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES18). http://indexive.com/Paper/157/detection-of-ddos-attacks-in-network-traffic-using-deep-learning.
17. A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet ofThings,” Future Generation Computer Systems, vol. 82, May2018,pp.761,768,2017,https://doi.org/10.1016/j.future.2017.08.043.
18. R. Doshi, N. Apthorpe and N. Feamster, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” 2018 IEEE Security and Privacy Workshops (SPW),SanFrancisco,CA,pp.29,35,2018,https://doi.org/10.1109/SPW.2018.00013.
19. Distributed denial of service attack (DDoS) definition.imperva.[Online].https://www.imperva.com/learn/application-security/ddos-attacks/Available:
20. K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 1-6, 2016, https://doi.org/10.1109/ISCO.2016.7727096.
21. Marchi D. L., and Mitchell L., "Hands-On Neural Networks: Learn how to build and train your first neural network model using Python," Packt Publishing, 2019.