PREDICTION OF DDoS ATTACKS USING DEEP LEARNING

Sasikala. C [1, a)] Jyothi. N, Mahesh Kumar. G, Meghana. V, Ashok.J[2,3,4,5, b)]

Author Affiliations

[1]Associate Professor Srinivasa Ramanujan Institute of Technology Anantapur, Andhra Pradesh, 515001, India

[2,3,4,5]Srinivasa Ramanujan Institute of Technology Anantapur, Andhra Pradesh, 515001, India

Author Emails

[1)]sasikala.cse@srit.ac.in

[2)]jyothinossam2002@gmail.com

[3)]maheshkumargodela@gmail.com

[4)]valasameghana@gmail.com

[5)]ashokjalipalli@gmail.com

Abstract. In recent years, Internet services have been increased in public and business ventures for production tasks. So internet applications need a lot of security to secure the data of other businesses and also itself. DDoSattacks are major security risks in the application environment. It happens by sending thousands of requests to flood the server and prevent it from processing requests. DDoS attack is a significant cybersecurity challenge that makes a particular system or network outof reach and unusual for some time. It affects the server's resources. The proposed system is used to detect such types of attacks by utilizing LSTM algorithm and a highlevel of accuracy. Hence, this work aims to solve this issue by applying a LSTM algorithm with a high degree of accuracy to detect thesetypes of assaults. The suggested technique, which has a 93% accuracy rate in identifying DDoS attacks, will be evaluated and simulated using Python and it is compared with the existing machine learning algorithms.

Keywords—Deep-Learning, Long-short-term memory (LSTM), Distributed-Denial-of-Service (DDoS) attacks.

INTRODUCTION

An intention to attempt to impede the regular operations of a network by flooding the target server or the surrounding infrastructure network with massive traffic is known as a DDoS assault. The success of DDoS attacks or assaults begins from the capacity to leveragethe large number of compromised computer systems as attack sources. Machines that are networked and have IoT devices could be deemed as exploited machines. At a high level, a denial-of-service attack (DDoS) might be likened to unexpected traffic that closes highway and prevent regular traffic from getting to its intended endpoint. DDoS assaults make use of computer networks that are online.

These networks contains of computer systems and various devices, including IoT devices, that been compromised by malware,which giving chance by allowing attackers to manipulate them remotely. Individually, these compromised devices can also be called as bots , and when grouped together, they form a botnet. Once the botnet is established, an attacker can exert control by issuing remote instructions to each bot, as illustrated in Figure 1. Sending queries to IP address of targeted server, every bot deployed in a botnet attack has the potential to inundate network, resulting in DoS for legitimate traffic. Differentiating between malicious and lawful traffic poses a challenge, as each bot functions as an Internet device.

The most noteworthy sign of a DoS assault is when an website suddenly becomes unreliable or else slow. However, since several factors, such a real traffic increase, which can cause to performance problems. You can identify some of these particular indicators of a DDoS assault with the aid of trafficanalytics tools. Unusual volumes of traffic coming froma one IP address, a severe flood of traffic from users with common device types, geo-location settings, or web versions, or an unaccounted spike in requests to single page are all signs of suspicious activity. Uncommon traffic patterns, such spikes at large number of times of the day or patterns that are out of ordinary (like a sharp increase of message for every 10 minutes).

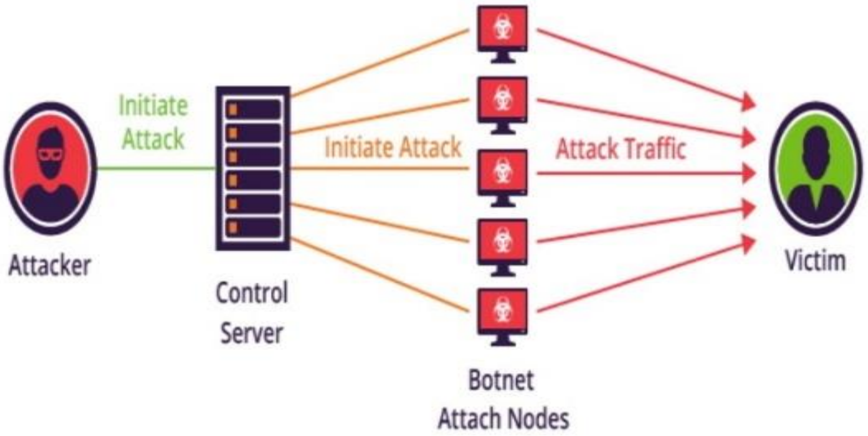

FIGURE 1. DDOS Attack using Botnet [13]

Some of the famous DDoS attacks on some organisations such as on 28 Feburary 2018. The largest DDoS attack was launched against GitHub, a well-known online code management site utilized by millions of developers. The platform was not ready for the enormous amount of traffic, which was peaked at a record-breaking of 1.3 terabits per second, even though it was accustomed to high levels of traffic. The GitHub attack used a technique called memcaching, it is a database caching solution meant to speed up networks or websites, rather than botnets. After successfully impersonating GitHub, the attackers significantly increased the volume of traffic going to the platform. Thanks to the DDoS protection solution that GitHub was utilizing, the attack was contained and prevented from spreading in less than ten minutes after it started.[14]

October 2016 saw the second-largest DDoS attack against major DNS operator Dyn. The hack caused significant disruption, by bringing down websites of over 80 of the organisation’s clients, including Amazon, Netflix, Spotify, Twitter, and PayPal. Hackers built a vast botnet of 100,000 IoT devices to execute their attack using a malware known as Mirai. Radios, smart TVs, and printers were among the gadgets that were set up to bombard Dyn with requests and cause traffic congestion. Approximately 14,500 domains stopped using Dyn's services immediately after the attack, which is estimated to have caused $110 million in damage even though it was contained in a single day.[14]

Ransomware and DDoS assaults were identified as the top two threats affecting businesses in 2018 by the UK's Crime Agency. They saw a sharp rise in attacks and recommended that organizations take urgent action to fortify themselves against this escalating danger.

This comprehensive list underscores the capacity of DDoS attacks to disrupt complete corporate website, network, and, as exemplified by the Dyn incident, potentially impact the entire internet. Businesses ought to think about utilizing a DDoS protection service, which can identify unusual traffic patterns and divert DDoS attacks off the network. Additional security precautions include using firewalls, VPNs, anti-spam software, and additional DDoS defense layers to safeguard network infrastructure.

Real-time of attacker disrupting user

DDoS attacks involves the malicious efforts for overwhelming the server or network with an excessive traffic, causing disruption and rendering the services inaccessible to legitimate users. The dynamic and distributed nature of cloud infrastructures further complicates the detection and mitigation of such attacks. Traditional security measures, while effective to some extent, are often insufficient in addressing the evolving sophistication of DDoS attacks.

The swift expansion of cloud computing in recent years has transformed how organizations handle and implement their IT infrastructure. The scalability, adaptability, and cost-effectiveness offered by cloud environments make them a compelling option for hosting crucial applications and services. Nevertheless, this extensive integration has brought about an increasing threat landscape, and DDoS attacks have become a significant challenge.

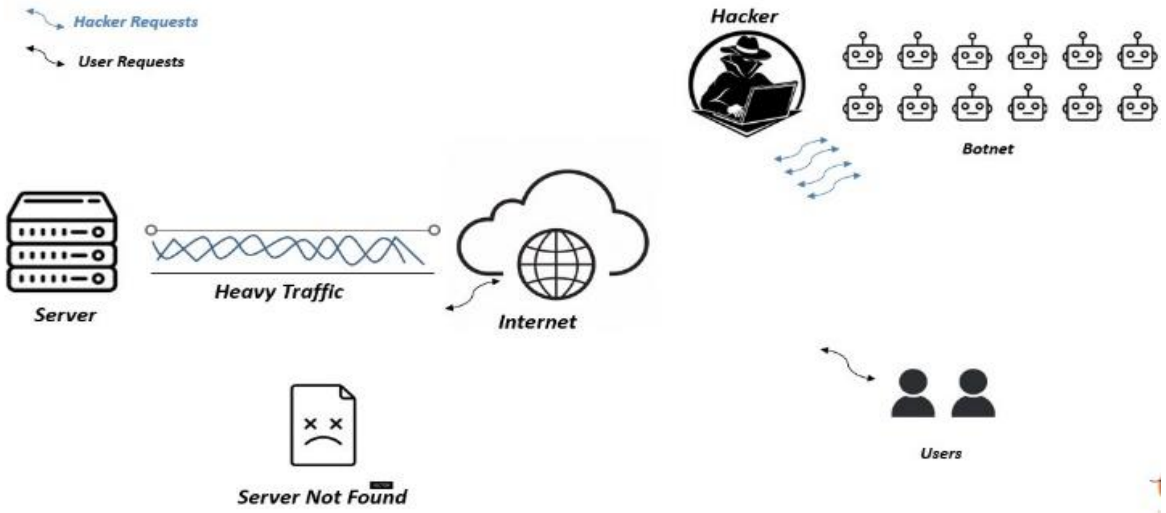

FIGURE 2: DDoS attacker disrupting user

The Figure 2 explains how the attacker attacks the network using a botnet and disrupts the usage of the normal user to access the server. By using botnet attackers increase the traffic over the internet and server, which makes the user unable to reach the server.

Deep Learning

This work focuses on leveraging of the power DL techniques for prediction and early detection of the DDoS attacks in application environments. Deep learning, a subset of machine learning, has demonstrated remarkable capabilities in extracting intricate patterns and features from complex data sets. By harnessing the inherent adaptability of deep learning algorithms, this project seeks to enhance the ability to identify and respond to the DDoS threats in real-time, thereby fortifying the security posture of cloud-based systems.

The objectives of the study encompass the development of a robust deep-learning model trained on historical data to recognize subtle patterns indicative of impending DDoS attacks. Additionally, the project will explore the integration of anomaly detection mechanisms to augment the model's ability to discern abnormal network behavior. The ultimate goal is to create an intelligent and proactive defense system capable of predicting and mitigating DDoS attacks before they can inflict significant damage. The objectives of the paper is three methodologies:

i. To develop a Deep Learning model (LSTM) to detect the attack.
ii. To compare the model with the Machine Learning models.
iii. To create a model which can be used for real-time intrusion detection of DDos attacks.

Through this work, aspire to contribute to the advancement of security by providing a predictive framework that empowers organizations to safeguard their critical assets and ensure uninterrupted service delivery in the face of evolving cyber threats. The outcomes of this project hold the potential to redefine the landscape of DDoS defense in the cloud, fostering a more resilient and secure digital environment for businesses and individuals alike.

LITERATURE SERVEY

It is unimaginable that a single attack could result in so significant damage to a computer system or network. However, due to its nature, DDoS will actually bring down the entire network. Its prevention is consequently very difficult to achieve. As a result, there is a huge demand for effective frameworks for DDoS attack detection. Several writers have developed several approaches to identify DDoS attacks in response to this demand. A few of them are detailed it has advantages and disadvantages:

Manju Khari, Rajiv Singh Ankit Agarwal.[1] Efficiently detecting potential threats while minimizing false alarms poses a challenge for many existing methods. Deep learning techniques prove to be effective in addressing this issue by categorizing both normal and attacked information. This research article introduces a novel approach called FS-WOA–DNN to effectively mitigate DDoS attacks. Initially, the input dataset undergoes a pre-processing step where a min–max normalization is employed to bring the inputs within specified range. Subsequently, the normalized data is given as input into proposed FSWOA to identify the optimal set of the features, facilitating to the classification process. These selected features are then fed into a DNN classifier to distinguish in between normal and attacked data.

Rami Khrais, and Abdulrahman Yateem Mohammad Shurman.[2] The paper introduces two approaches for the identification of DDoS attacks in the IoTs. The initial method employs a hybrid IDS to identify IoT-DoS attacks, while the second model utilizes deep learning models, specifically based on LSTM, trained using the most recent dataset relevant to DDoS of this nature.

LiXinlong and Chen Zhibin, [3]. In the study, a Hybrid Deep Learning approach is employed to identify malicious web traffic such as DDoS attacks, regulating the information flow toa server while leveraging interdependencies among different elements within a data stream. The proposed model introduces an innovative Hierarchical Temporal Memory (HTM) hybrid architecture. The functionality of model is primarily based on neocortex, a segmentof cerebral cortex responsible for fundamental brainfunctions, encompassing sensory perception, language comprehension, and movement control.

Sarem, M & Dong, S. [4] The persistence of DDoS attacks has posed a continualthreat to network availability over the years, with existing defense mechanisms proving insufficient. However, theadvent of SDN offers a novel approach to addressing DDoS. This paper introduces two detection methods within the SDN framework. The first method is for leveraging the degree of the DDoS attack for identification, while the second methodemploys an enhanced KNN algorithm, utilizing ML techniques for detection. Theoretical analysis and experimental results on datasets demonstrate the superior efficacy of our proposed methods in detecting DDoS attacks compared toalternative approaches.

Jain, R & Abbas, K., [5] Recently, researchers andindustries has widely embraced SDNs and cloud computing; however, their broad acceptance has been hindered by security threats. The evolution of processing technologies has empowered attackers to escalate their efforts, exemplified by the transition from DoS attacks to more sophisticated DDoS attacks, which conventional firewalls struggle to detect. This paper delves into current landscape of DDoS attacks within SDN and cloudcomputing frameworks, with a specific focus on analyzing their architectures. Additionally, weprovide an overview of existing research efforts and highlight open challenges related to detection and mitigation of DDoS threats in these environments.

PROPOSED SYSTEM

In this proposed model it is an innovative application that can be considered a highly useful system, as it addresses the limitations commonly encountered with traditional and other existing methods for DDoS attack detection. This research aims to create a efficient and dependable approach for precisely identifying impact of DDoS attacks. The model design utilizes a robust algorithm within a Python-based framework, incorporating the integration of LSTM neural-networks to enhance its capabilities. Figure 3 shows the overall architecture of the proposed model. Figure 5 shows the model training and testing of the proposed system.

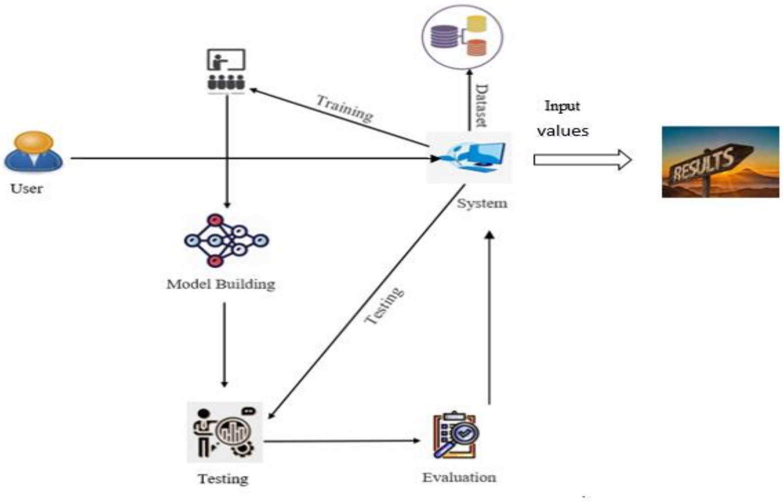

FIGURE 3. System Architecture

User approach

- Upload Dataset**:** In this module, users have the capability to upload their dataset, typically in a specified format (e.g., CSV, Excel, or database connection). The system should provide clear instructions on the accepted data format and structure, ensuring a seamless data upload process.
- View Dataset: Users can view the dataset they have uploaded. The system may provide features for data visualization, filtering, and summary statistics to help users understand and explore the dataset before initiating the prediction process.

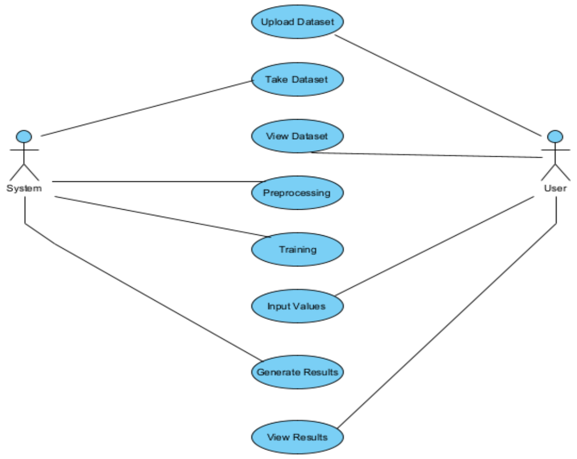

FIGURE 4. Use Case Diagram

- Input Values for Prediction: Users need to provide input values relevant to the prediction task. These inputs could include specific data points or variables necessary for the model to make predictions. The system should guide users on what input is required and validate the inputs to ensure they meet the necessary criteria.

System approach

- Take Dataset: The system takes the dataset uploaded by user and stores it securely. It performs data integrity checks and ensures that the dataset is available for further processing.
- Preprocessing: In the preprocessing phase, the system cleans and prepares the data for model building. This involves handling missing values, data transformation, normalization, and feature engineering. It is a critical step to ensure the dataset is ready for training.
- Training: The system utilizes Deep Learning techniques to build a predictive model based on preprocessed dataset. This process might include dividing the dataset into training and testing subsets, choosing a suitable algorithm, and then training the model using the designated training data.This model is then evaluated of its performance on the testing data.
- Generate Results: Once the model is trained, the system uses it to generate results. For a DDoS attack prediction system, this could mean evaluating whether the input values provided by the user are indicative of an attack or not. Results may be presented to user in an user-friendly format, such as binary classification (e.g., "Attack Detected" or "No Attack Detected") or with probability scores. Users may also receive insights or visualizations that help them understand the model's decisions. Figure 4 shows the use case diagram of the model which give an overview approach of the user and the system.

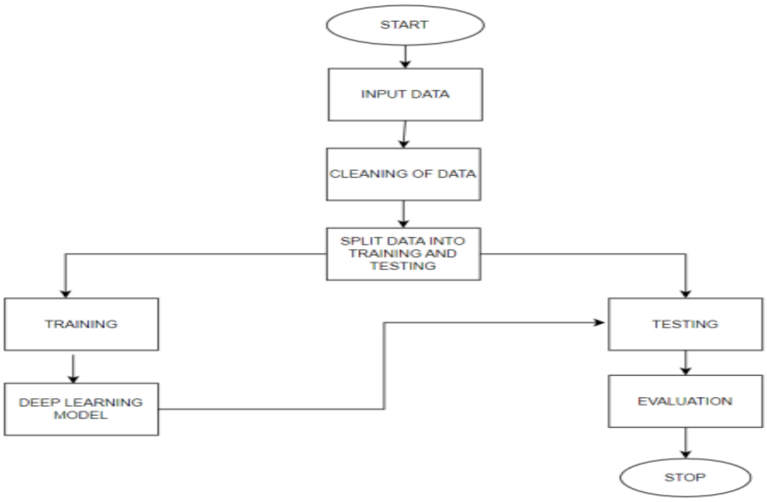

FIGURE 5. Architecture of LSTM Proposed system

IMPLEMENTATION

The functioning of a Recurrent Neural Network is based on the concept of retaining the output from a specific layer and reintroducing it as input, enabling the model to predict subsequent layer outputs, as illustrated in Figure 6.

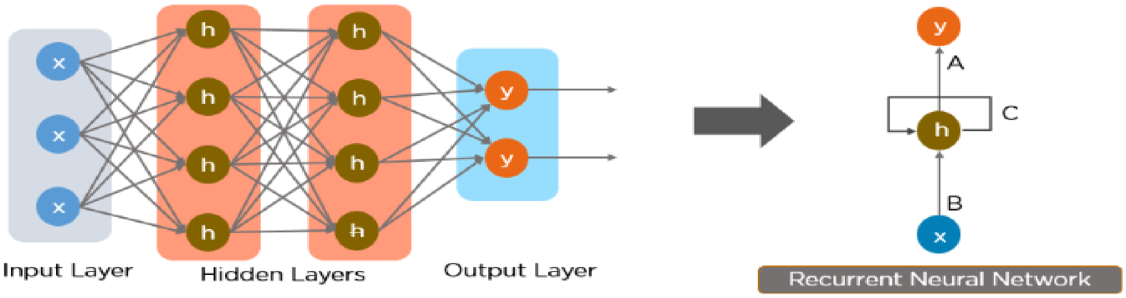

FIGURE 6. Simple Recurrent Neural Network

Feed-Forward Neural Networks:
Figure 7 shows a simplified representation ofa feed-forward-neural-network. A feed-forward NN restricts information flow to only one direction: forward from the input to output nodes via the hidden layers. The network does not contain any cycles or loops.

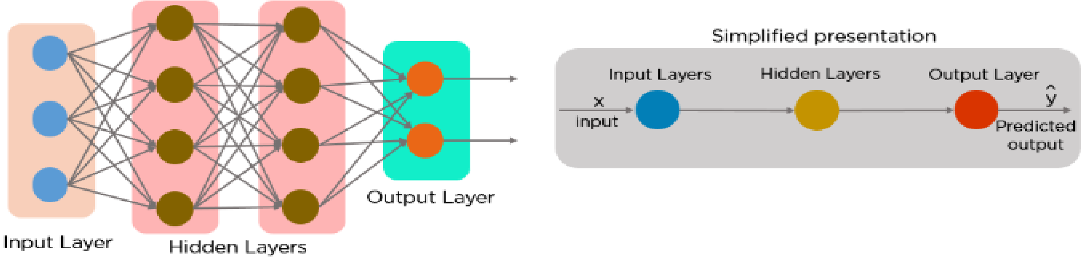

FIGURE 7. Feed-forward NN.

The inception of RNNs stemmed from challenges encountered in feed-forward neural networks, specifically their limitations in handling sequential data. Unlike feed-forward networks that focus solely on the current input without retaining information from previous inputs, RNNs address this issue by offering the capability to manage consecutive data and recall past inputs. Both the current inputs and previously received input can be handled in sequentially by an RNN. Because RNNs have internal memory, they can retain earlier inputs.

Working of LSTM Model

The development of recurrent neural networks stemmed from several challenges encountered in feed-forward neural networks.Unable to handle sequential data, it only considers the present input and lacks the ability to retain previous inputs.For these problems, the Recurrent-Neural Network (RNN) provides the answer. Both the current input and previously received input can be handled sequentially with RNN, cause RNNs have internal memory, they can retain earlier input.Recurrent Neural Networks (RNNs) share similarities with traditional neural networks but excel in capturing long-term dependencies, especially in task involving the sequence prediction. Unlike neural networks that focus on individual data points, LSTM stands out for its capacity to understand entire sequences due to the incorporation of feedback connections.

- A memory cell that sustains its state across time, referred to as a "cell state," plays a pivotal role in LSTM model. The horizontal line which that pass through the above or top of cell in LSTM cell as\ in Figure 8 represents the cell state. It might be seen as an information conveyor belt that information just moves across, unaltered.

- In LSTM, gates control the addition and deletion of data from the cell state. Information can optionally enter and exit the cell through these gates. To facilitate its operation, the system incorporates a sigmoid neural layer in conjunctionwith pointwise multiplication operation.

- Typically, the remember vector can also be refer as the forget gate. The forget gate's output multiplies 0 to a matrix point to notify the cell state what data to ignore. Information is retained if output of forget gate is 1, describe the status of the cell state..The prior hidden state and the weighted input/observation are subjected to the sigmoid function derived from the equation 1.

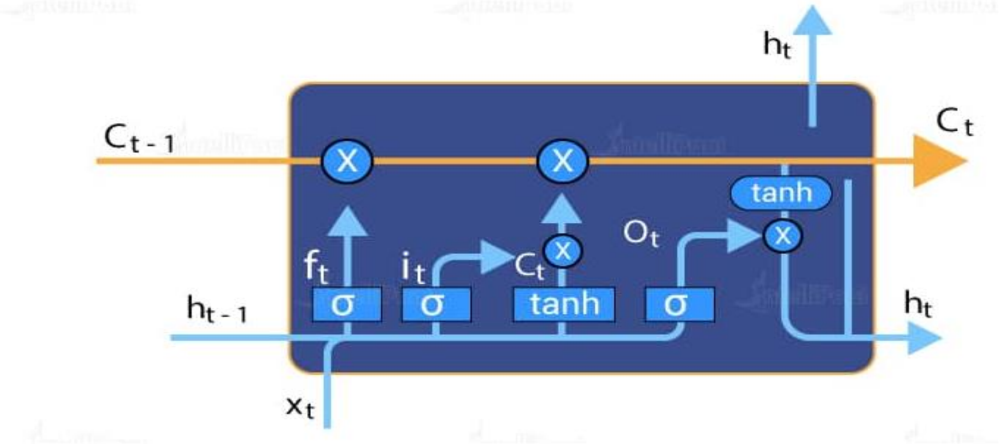

FIGURE 8. Single LSTM cell

- The input gate is the common term for the save vector. Where data goes into the long-term memory or cell state is decided by these gates. The activation functions for each gate are the key components. The input gate has a range of [0,1] and is a sigmoid function. Since the cell state equation is a summation of the preceding cell states, the sigmoid function by itself can only accumulate memory; it cannot erase or forget information.
- A floating number that can only be added between [0,1] will never be zero, turned off, or forgotten. Tanhx activation function is present in the input modulation gate for this reason. Tanh permit the cell state to forget the memory and has a range of[-1, 1]. The output gate is the common term for as focusvector. Where value out of all available valuesfrom the matrix.
- The forget gate is first sigmoid activation function. Which data from previous cell state(Ct-1) should be ignored. Our input gate is the firsttanh and second sigmoid activation function. Which data ought to be erased or preserved in cell state? The output gate, or last sigmoid, indicates which data should proceed to the following hidden state.
- Data Pre-Processing activation-function-formula:

$$f(t)=\sigma(W_f[h_t-1,x_t]+b_f) \quad ---(1)$$

$$i(t)=\sigma(W_i[h_t-1,x_t]+b_i) \quad ---(2)$$

$$o(t)=\sigma(W_o[h_t-1,x_t]+b_o) \quad ---(3)$$

$$f(xt)=1/(1-e^{\alpha xt}) \quad ---(4)$$

$$tanhx=(2/(1+e^{-2x})) \quad ---(5)$$

RESULT ANALYSIS

The entire set of outcomes from our suggested models is included in this section. Each and every result is presented in detail using figures along with an explanation of the findings.

Data Pre-processing

This is a crucial and time-consuming step in data analysis process. Here, the data will be filtered to remove unnecessary information and transformed into high-quality information. For this action, the missing values are replacing values in the data that are not relevant to our experimental investigation utilizing statistical approaches. For the first phase of the examination, this is a requirement for all data analyses. We will then be able to transform information into a trustworthy format. to look at the graphical form's value and information. For oversampling in this paper we used RandomOversampler. Figure 9 represents the heat-map of representing the missing values in the dataset. The findings indicate that there are no extraneous values requiring elimination from the dataset.

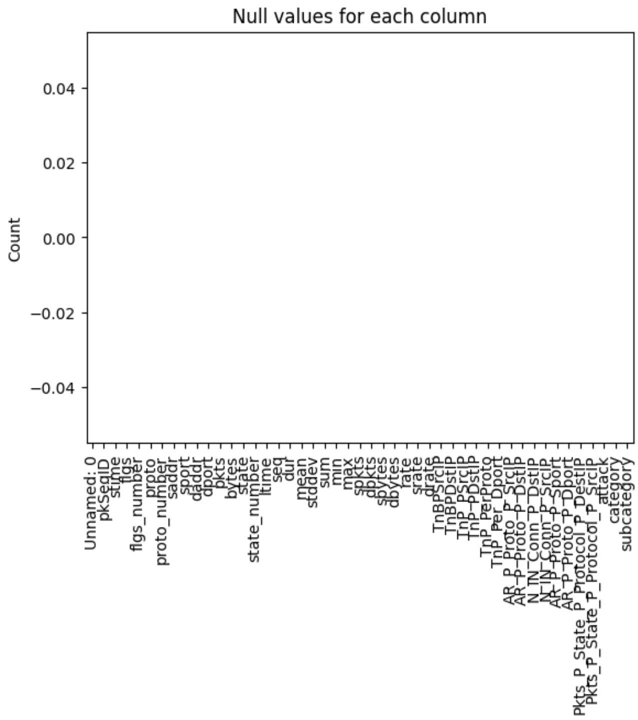

FIGURE 9. Heat-map of missing values

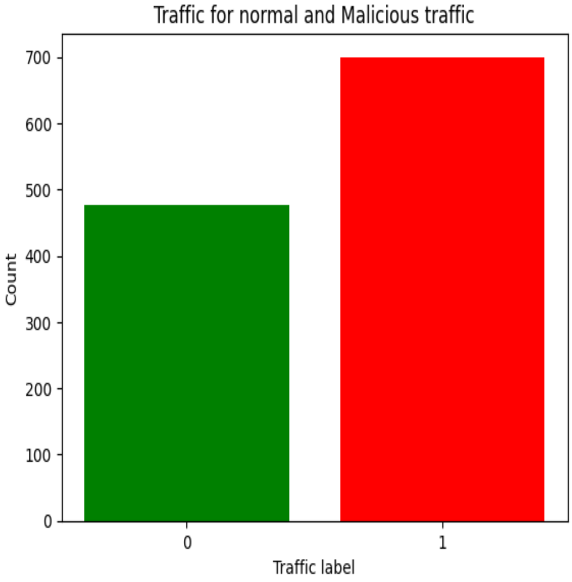

FIGURE 10. Attacks

Computers cannot process letter data because their understanding is sporadic. Additionally, in this instance, the computer algorithms are unable to comprehend the information in letter form. Thus, it's crucial to transform this information into a digital format for the suggested model to comprehend. Deep learning is used to create the label encoder, which we can then shape into the desired form. Our dataset, which has been transformed to numerical form, is fully presented in the graphical Figure 10.

The proposed model is developed with the LSTM algorithm which has an accuracy of approximately 93%. The precision of 93.39%, recall of 92.33% and F1 scores of 91.3% are calculated using the table of confusion values from confusion matric.

$$\text{accuracy} = \frac{TP+TN}{(TP+TN+FP+FN)}$$

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

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

$$F_1\,\text{–score} = 2.\,\frac{Precision\,.\,Recall}{Precision+Recall}$$

According to the analysis, the LSTM model demonstrates superior accuracy in comparison to traditional Machine Learning models. The suggested model achieves an accuracy rate of 93%, surpassing Gradient Boosting with 88% accuracy and Decision Tree algorithm, which exhibits an accuracy of 80%.Table 1 shows the values of each model that occurred during the training of the models. Figure 13 is the graphical representation of each model of their metrics.

TABLE 1. Comparision of Metrics of LSTM model with Machine Learning models.

Algorithms	Accuracy	Precision	Recall	F1-score
LSTM	93	93.39	92.33	91.33
Gradient Boosting	88	88.72	89.61	90.61
Decision Tree	80	91.7	90.2	90.07

Figure 11 shows result of LSTM model and Gradient Boosting and Figure 12 shows the results of LSTM model and Decision tree. The graphical representation shows the comparision of different metrics.Hence, the proposed system is more accurate than Machine Learning algorithms

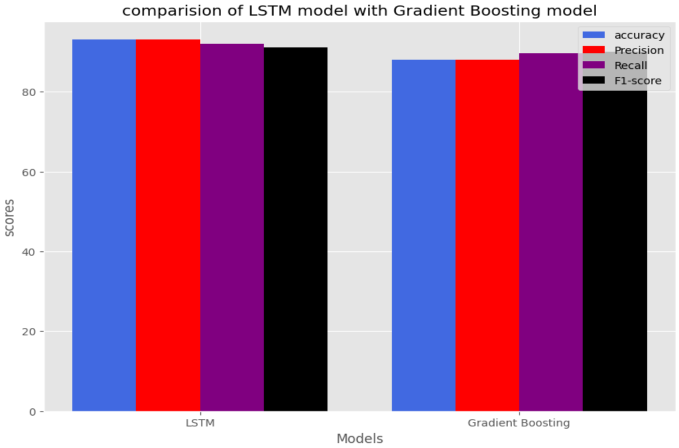

FIGURE 11. Comparision of LSTM model with Gradient Boosting model

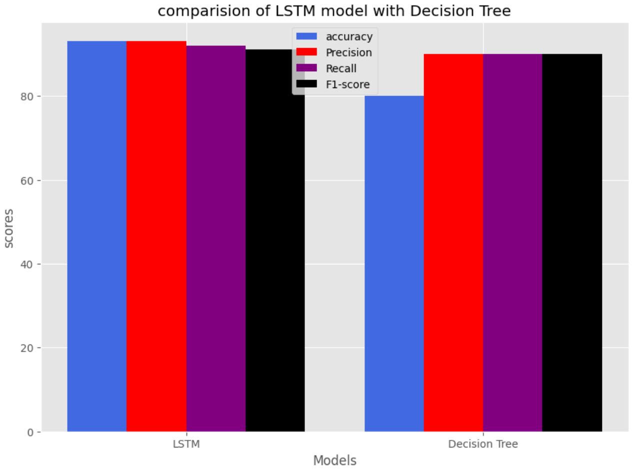

FIGURE 12. Comparision of LSTM model with Decision Tree model

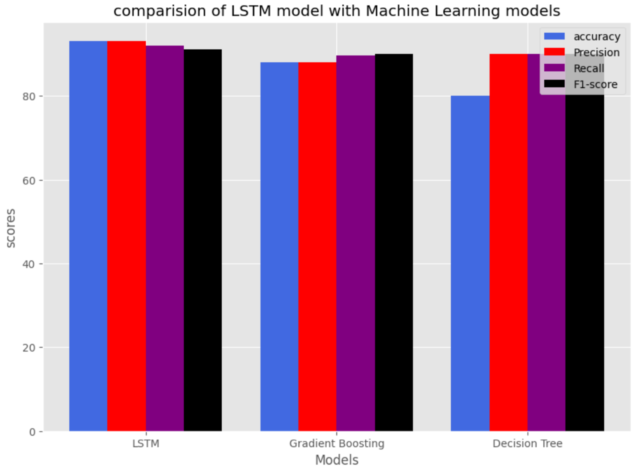

FIGURE 13. Graph between the deep learning model and Machine Learning models.

CONCLUSION AND FUTURE WORK

In the contemporary landscape, DDoS attacks pose significant threats. To mitigate the associated losses by promptly identifying targeted networks, we have developed a model leveraging the LSTM algorithm. This model exhibits a remarkable accuracy of 93%, surpassing established machine learning counterparts such as Decision Tree and Gradient Boosting algorithms. Implemented in Python, our solution not only enhances detection capabilities but also operates seamlessly in real-time network environments, providing a superior and intuitive solution. To ascertain whether or not the network is under assault, the system probably collects user data.For Future work, this model can be enhanced to cloud environment as the cloud is the most targeted place by the DDoS attackers which may affect the organizations.

REFERENCES

1. Ankit Agarwal, Manju Khari, Rajiv Singh, "Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application", Springer Nature, pp. 1-21, 4 February 2021.
2. Mohammad Shurman, Rami Khrais, and Abdulrahman Yateem, "DDoS and DDoS Attack Detection Using Deep Learning and IDS ",pp. 1-8, The International Arab Journal of Information Technology · July 2020.
3. Li Xinlong and Chen Zhibin, " DDoS Attack Detection by Hybrid Deep Learning Methodologies", pp. 1-8**,** Hindawi Security and Communication Networks, May 2022
4. Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048.
5. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in S DN and cloud computing environments. IEEE Access, 7, 80813- 80828.
6. G u, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.
7. C M Nalayinil, Dr. Jeevaa Katiravan, "Detection of DDoS attack using Machine Learning Algorithms", Journal of Emerging Technologies and Innovative Research(JETIR), vol.9, pp. 1-10, July 2022.
8. Marram Amitha, Dr. Muktevi Srivenkatesh, "DDoS Attack Detection in Cloud Computing Using Deep Learning Algorithms", pp. 1-10, Intelligent Systems and Applications in Engineering, 2023.
9. Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.
10. Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.
11. Meti, N., Narayan, D. G., & Baligar, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In 2017 international conference on advances in computing, communications and informatics (ICACCI) (pp. 1366-1371). IEEE.

12. 15th International Symposium on Pervasive Systems, Algorithms and Networks IEEE DDoS Attack Identification and Defense using SDN based on Machine Learning Method, 2018

13. JamesMacKay https://www.metacompliance.com/blog/cyber-security-awareness/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them