IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13343

Detection of DDoS Attack Using Deep Learning

Sharan K R[1], Shreekavya C H[2], Rony Dominic[3], Soniya A Gunagi[4], Vasudha G Rao[5]

Student, Dept. of Artificial Intelligence & Machine Learning, Mangalore Institute of Technology & Engineering, Moodabidre, India[1-4]

Professor, Dept. of Artificial Intelligence & Machine Learning, Mangalore Institute of Technology & Engineering, Moodabidre, India[5]

Abstract: A Distributed Denial-Of-Service (DDoS) assault is a hostile activity that aims to overload a server, service, or network with excessive network traffic, rendering it unusable. The fact that attack patterns are constantly shifting, cyber offense techniques are developing quickly, and cyber offense materials are freely available on the dark web have made this a difficult task. DDoS assaults have the potential to seriously impair online services, resulting in lost profits, harmed reputations, and dwindling client confidence. Additionally, it may lead to overheating or power outages, which could harm infrastructure. Taking into account all of these factors, this research focuses on predicting and classifying DDoS attacks through the analysis of network traffic data using a deep learning technique to automate the manual process. In the end, this can reduce human error in the detection process and save time and effort. This project trains the "DDoS Evaluation – CICDDoS2019" dataset using the power of the Long Short Term Memory(LSTM). To improve the accuracy of anomaly detection, the LSTM is trained in an unsupervised environment to recover encoded data. In a monitored setting, the LSTM is trained to categorize network traffic data into DDoS attacks.

Keywords: Distributed Denial-Of-Service (DDoS), Deep Learning, Long Short Term Memory(LSTM)

I. INTRODUCTION

DDoS attacks cause a network's servers and resources to become less available by flooding the network with traffic from multiple devices located in different locations. This makes it challenging to identify DDoS assaults, which only seek to overload the target server without stealing any data. Although DoS and DDoS are two distinct attack techniques, the attacker's ultimate goal is always the same. One victim and one attack computer are used in denial-of-service attacks. DDoS assaults, on the other hand, rely on a larger number of compromised bots to perform the tasks concurrently in order to infect the target server, making it harder for authorized users to access the services.

In order to take advantage of weak devices and make them into botmasters, attackers created a botnet. A botnet, often known as a zombie army, is an assemblage of compromised web browsers that may be remotely managed without the owner's awareness by the introduction of malware into each device. When bot computers are used in DDoS assaults, their resources may become overburdened, causing them to crash and operate poorly.

A botmaster searches for weak points in devices and uses malware to infiltrate the systems. Once the hacker has penetrated enough devices, they order the attack to begin. Each system then begins to overload the target system to networks with requests, which causes slowdowns or outright failures. Although they frequently depend on signature-based security and find it difficult to adjust to changing threats, antivirus programs and systems for intrusion detection (IDS) are frequently utilized for defense. Determining malicious network traffic in real time is essential.

The dynamic nature of network traffic abnormalities, however, poses a challenge to current approaches. By learning the temporal characteristics of both benign and DDoS traffic flows, our system shortens processing times and speeds up detection.

It provides an effective solution for resource-constrained online environments and improves cybersecurity by tackling the dynamic nature of cyberthreats. In this study, we detect and classify DDoS attacks using long-short term memory (LSTM). Because they have internal memory, RNNs are powerful and durable neural networks that rank among the most efficient algorithms. They make use their own internal memory to recollect salient features of the information they are given. For the processing, classification, and prediction of time series of data with ambiguous temporal spans, LSTM is a good choice.

DOI: 10.17148/IJARCCE.2024.13343

II. LITERATURE REVIEW

Hybrid deep learning approach in a supervised environment [1] aims to automate DDoS attack classification, enhancing efficiency and accuracy while reducing manual effort. By leveraging the LSTM autoencoder and LSTM multi-class classifier, the proposed system effectively trains on the "DDoS Evaluation – CICDDoS2019" dataset. The LSTM autoencoder refines anomaly detection accuracy through unsupervised reconstruction of encoded data, while the LSTM multi-class classifier accurately identifies DDoS attacks in a supervised setting. Through extensive experiments involving hyperparameter tuning, architectural adjustments, and preprocessing techniques, showcasing notable improvements in accuracy, precision, recall, and F1 Score. Additionally, the research identifies areas for future advancement.

The multilayer perceptron (MLP) classifier [2] enhances novel application layer DDoS attacks by analyzing the characteristics of incoming packets, including the size of HTTP frame packets, the number of Internet Protocol (IP) addresses sent, constant mappings of ports, and the number of IP addresses using proxy IP. We analyzed client behavior in public attacks using standard datasets, the CTU-13 dataset, real weblogs (dataset) from our organization, and experimentally created datasets from DDoS attack tools: Slow Lairs, Hulk, Golden Eyes, and Xerex. A multilayer perceptron (MLP), a deep learn-ing algorithm, is used to evaluate the effectiveness of metrics-based attack detection. The per-formance of our proposed technique provided the lowest value of false positives of 2.11% com-pared to conventional classifiers, i.e., Naïve Bayes, Decision Stump, Logistic Model Tree, Naïve Bayes Updateable, Naïve Bayes Multinomial Text, AdaBoostM1, Attribute Selected Classifier, Iterative Classifier, and OneR.

Gradient Boosting Decision Tree (GBDT) parallel ensemble learning method and light-weight usable deep learning model [3] introduces an efficient method for early anomaly traffic detection, focusing on profiling traffic patterns from the first few bytes of each flow. It employs two deep learning models: a Gradient Boosting Decision Tree (GBDT) parallel ensemble technique and a lightweight Convolutional Neural Network (CNN) model leveraging CNN properties. The outputs from both models are combined using an add function to merge spatial and temporal features, resulting in a hybrid model capable of accurately identifying malicious or benign traffic flows. This hybrid ensemble learning approach showcases enhanced detection accuracy compared to existing techniques.

III. SCOPE AND METHODOLOGY

Scope

The main aim of the project it developing and implementing deep learning algorithms to analyze CICDDoS2019 for the detection of DDoS attacks using deep learning. Taking the network traffic information and using data cleaning and preprocessing techniques to determine the best features. Find abnormalities in the network traffic file and categorise them using deep learning techniques. DDoS assaults such as Syn Flood, LDAP, MSSQL, NetBIOS, BENIGN flow, and etc are categorised by this project. To make the dataset appropriate for a multiclass classification problem, balance it. Analyse the system's effectiveness and contrast the suggested strategy with the ones that are currently in use.

Methodology

The methodology for evaluating LSTM-based DDoS detection systems involves a structured approach to ensure the effectiveness and reliability of the model. It commences with meticulous data preparation, starting with the selection of a diverse and representative dataset containing both benign and malicious network traffic. Upon dataset import and distribution, attention is paid to ensure random distribution, mitigating potential biases. Subsequently, the dataset undergoes preprocessing techniques such as feature selection, label encoding, normalization, and reshaping. These steps aim to ensure data consistency and suitability for input into the LSTM model.

In the subsequent phase of LSTM model development, a sophisticated architecture is designed to effectively capture sequential patterns in network traffic data. Leveraging the Keras API for LSTM model development signifies a commitment to employing state-of-the-art approaches. Multiple hidden layers are incorporated to tap into the unique memory-retention capabilities of LSTMs, enabling the model to capture intricate sequential patterns. Components such as LSTM cells, memory cells, input gates, forget gates, and output gates are carefully implemented to facilitate information flow and retention across multiple time steps, ensuring the model's efficacy in analyzing network traffic.

Following model development, the training phase ensues, where the LSTM model learns to discern patterns and adapt to complexities present in the dataset. Hyperparameter tuning is conducted to optimize model performance, striking a balance between computational efficiency and accuracy. Convergence monitoring ensures that the model reaches an optimal state, poised for evaluation. Subsequently, model evaluation entails testing its performance on separate test datasets to assess its ability to generalize to unseen instances.

DOI: 10.17148/IJARCCE.2024.13343

Metrics such as accuracy and etc. are utilized to gauge the model's effectiveness in distinguishing between benign and malicious traffic, while overfitting checks ensure the model's resilience in real-world scenarios. Finally, upon successful evaluation, the trained LSTM model is deployed onto a production server, where its capability to analyze live traffic flows in real-time and detect DDoS attacks plays a pivotal role in proactive defense against evolving threats.

IV. DESIGN AND IMPLEMENTATION

This architectural diagram showcases a DDoS attack detection system powered by a Long Short-Term Memory (LSTM) model. It uses an LSTM network to classify DDoS attacks. It cleans and prepares CICDDoS 2019 data for training and testing the LSTM. The LSTM analyzes sequences to distinguish normal traffic, DDoS attacks (of various types), and anomalies, ultimately acting as a shield to identify and flag DDoS attempts.

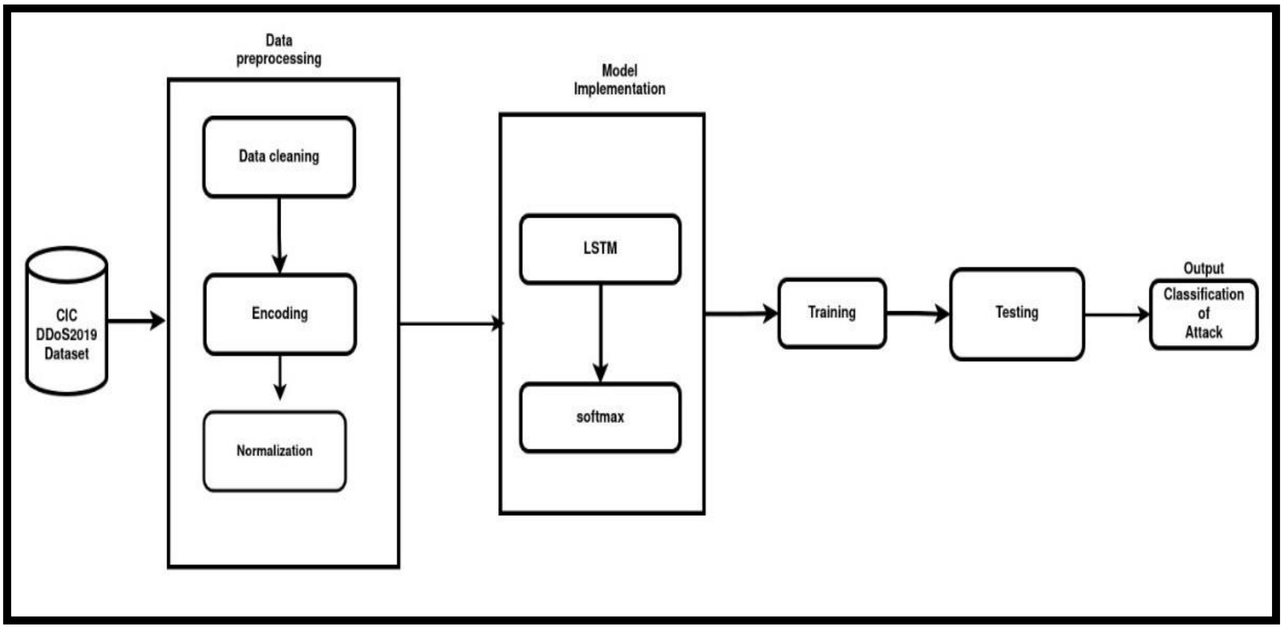

Fig 1. Architecture diagram

V. RESULT AND CONCLUSION

Result

Using the CICDDoS2019 dataset, our study sought to assess the effectiveness of deep learning models known as Long Short Term Memory (LSTM) in identifying and categorizing DDoS attacks. After extensive training and testing, we discovered that, when compared to the RNN model, the LSTM demonstrated exceptional classification accuracy of 91.58%. The RNN model performed relatively poorly, as evidenced by its accuracy of 42.38%. These results imply that the LSTM model might provide the best outcome for DDoS attack detection. Additionally, we were able to categorize various DDoS attacks, enabling users to become aware of them.

Conclusion

DDoS attacks pose a serious threat to the integrity of networks since they can cause significant interruptions as well as significant financial losses. With the use of deep learning methods like LSTM, this research aimed to fully utilize the potential of machine learning in order to develop a reliable system that could quickly identify and mitigate DDoS attacks in real-time.

To improve model performance, the dataset was first preprocessed by removing columns with single unique values and converting category labels into numerical forms. Standardization and normalization were then used. The main goal of the project was to build and train an LSTM model that was specifically intended to identify DDoS attacks by utilizing its ability to capture long-term dependencies in sequential data. By employing several LSTM layers and adding dropout layers to prevent overfitting, the trained model demonstrated promising performance metrics across both training and test datasets.

DOI: 10.17148/IJARCCE.2024.13343

REFERENCES

[1]. Goonathilaka, M.O., 2023. A Hybrid Deep Learning Approach for DDoS Attack Classification using Network Traffic Data Analysis (Doctoral dissertation, University of Westminster).

[2]. Ahmed, S.; Khan, Z.A.; Mohsin, S.M.; Latif, S.; Aslam, S.; Mujlid, H.; Adil, M.; Najam, Z. Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron. Future Internet 2023, 15, 76.

[3]. Fathima, A., Devi, G.S. and Faizaanuddin, M., 2023. Improving distributed denial of service attack detection using supervised machine learning. Measurement: Sensors, p.100911.

[4]. Aktar, S. and Nur, A.Y., 2023. Towards DDoS attack detection using deep learning approach. Computers & Security, 129, p.103251.

[5]. Alashhab, A.A., Zahid, M.S.M., Azim, M.A., Daha, M.Y., Isyaku, B. and Ali, S., 2022. A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. Symmetry, 14(8), p.1563.

[6]. Ramzan, M.; Shoaib, M.; Altaf, A.; Arshad, S.; Iqbal, F.; Castilla, Á.K.; Ashraf, I. Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm. Sensors 2023

[7]. Zhou, H., Zheng, Y., Jia, X. and Shu, J., 2023. Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN. Computer Networks, 225, p.109642.