DDOS Detection using Machine Learning

Tanisha Nagpal
AIT-CSE
Chandigarh University
21BCS5286@cuchd.in

Aaditya Singh
AIT-CSE
Chandigarh University
21BCS6750@cuchd.in

Disha Saini
AIT-CSE
Chandigarh University
21BCS6773@cuchd.in

Ishaan Shandilya
AIT-CSE
Chandigarh University
21BCS6777@cuchd.in

Abhishek
Ankur

AIT-CSE
Chandigarh University
abhishek.e12833@cumail.in

Abstract— Distributed Denial of Service (DDoS) attacks have emerged as a pressing threat in the digital landscape, compromising the availability and performance of online services. Traditional detection and mitigation strategies often fall short due to the evolving nature of these threats. This paper explores the application of machine learning (ML) techniques in developing robust DDoS detection systems. We discuss the fundamental concepts of DDoS attacks, the challenges in detection, and present various machine learning algorithms, feature selection methods, and evaluation metrics for DDoS detection systems. The effectiveness of machine learning approaches is illustrated through case studies and experimental results, highlighting their potential to enhance cybersecurity efforts.

The advent of the Internet of Things (IoT) and the expansion of online services have rendered network infrastructures increasingly vulnerable to cyber-attacks, particularly Distributed Denial-of-Service (DDoS) attacks. This review paper synthesizes recent advances in deep learning techniques for DDoS detection, focusing on Long Short-Term Memory (LSTM) models, their implementation, benefits, and potential compared to traditional machine learning methods. Machine learning offers a promising solution to address the evolving nature of DDoS attacks. By analyzing network traffic patterns and identifying anomalies, ML-based systems can effectively detect and mitigate these threats.

Keywords— ***Station announcements, natural language translation engine, Language diversity, accessibility***

I. INTRODUCTION.

Machine learning (ML) has emerged as a transformative solution to the challenges posed by Distributed Denial of Service (DDoS) attacks, which are becoming increasingly sophisticated and frequent. DDoS attacks aim to overwhelm a target—such as a server, service, or network—by flooding it with excessive traffic. This overload can cause the target resource to become slow, unresponsive, or even completely inaccessible. As cyber threats evolve, there is an urgent need for advanced techniques to preemptively identify and mitigate these attacks. This is where machine learning steps in, revolutionizing the way organizations defend their digital assets. One of the primary benefits of machine learning in the context of cybersecurity, particularly in identifying DDoS attacks, is its capability to analyze vast amounts of data in real-time. Traditional security systems often rely on predefined rules and thresholds to detect anomalies. However, these approaches can fall short, especially in the face of ever-evolving attack strategies. Machine learning, on the other hand, leverages data-driven methodologies to learn from historical traffic patterns and adaptively recognize when deviations from the norm occur. By analysing past incidents, machine learning algorithms create models that can be used to identify patterns that might go unnoticed by human analysts or conventional detection systems.

The learning process begins with training the model on historical data, which includes both normal and attack traffic patterns. During this phase, the algorithm identifies various features of the data that are relevant for classification. These features might include the source of traffic, the volume of packets sent, the frequency of requests, and other contextual information. Once trained, the algorithm can autonomously monitor live traffic and identify fluctuations that suggest a potential DDoS attack is underway. This ability to discern subtle shifts in behavior enables organizations to detect attacks early and respond more effectively.

What makes machine learning particularly effective is its use of advanced techniques, such as supervised and unsupervised learning. In supervised learning, the model is fed labeled data, meaning that it learns from examples of known traffic patterns associated with attacks versus those considered normal. This helps to build a robust model that can classify new, unseen data accurately. On the other hand, unsupervised learning does not rely on labeled data. Instead, it identifies patterns and anomalies in datasets by detecting outliers. This approach is especially useful in identifying novel attacks that may not have been seen before, thus expanding the capacity to thwart future threats.

Moreover, the evolution of ensemble methods, which combine multiple models to improve accuracy, enhances the efficacy of detecting DDoS attacks.

By integrating different algorithms, organizations can achieve more reliable detection, reducing false positives while ensuring genuine threats are flagged without delay. This multidimensional approach directly translates into improved response strategies and fortifies the overall cybersecurity posture of an organization.

Another significant advantage of ML in DDoS mitigation is its efficiency in automating responses. Once a potential attack is detected, predefined actions can be initiated automatically, such as throttling bandwidth for suspicious sources or rerouting traffic through scrubbing centers. This rapid response can significantly diminish the impact of an attack, ensuring that business operations remain uninterrupted.

In conclusion, the application of machine learning in identifying DDoS attacks is a testament to the power of modern technology in tackling complex cybersecurity challenges. By harnessing data-driven approaches to discern patterns that escape traditional detection methods, machine learning not only enhances the speed and accuracy of threat detection but also paves the way for more robust and adaptive security measures. As cyber threats continue to evolve, machine learning will undoubtedly play a critical role in the future of cybersecurity, ensuring that organizations can defend their digital landscapes with greater confidence and resilience.

II. LITERATURE SURVEY.

[1] This chapter outlines a brief overview of DDoS attacking techniques and solutions in an SDN environment. First of all, we provide an overview of SDN and the advantages it has over traditional networks. Further, different vulnerabilities in SDN are being discussed along with DDoS attack. Then we present some characteristics that SDN poses to defeat this massive DDoS attack. Various taxonomies of DDoS attacks which affect the SDN environment are also discussed. We end up here with some directions for future research that could be a crucial idea to defend such attacks in the near future.

[2] The DRDoS attacks use DNS servers for reflecting traffic against a target overpowers it by providing relevant response traffic without any direct communication with the attacker and the victim. This article would therefore entail an examination of the mechanics of the attack, amplification techniques that are used in DNS servers, and vulnerabilities that often prevail in DNS services. It would discuss mitigation procedures, including filtering methods, traffic analysis, and anomaly detection, that could show techniques that would make robust configurations of the DNS servers.

[3] To propose a cascade intrusion detection method which is mainly based on distributed machine learning and deep learning so that it may be exploited to High Dimensional Massive Data. Exploit deep learning on Spark's driver side to learn only the hidden features of attack samples and Adaptive Synthetic Sampling (ADASYN) to avoid the polarization of the classifier, which reduces coupling between normal and attack events besides reducing data processing time and transformation time.

[4] This paper investigates the detection of DDoS attacks in software-defined networks, especially on the pros and cons of separating the control and data planes of SDNs. The authors present machine learning and deep learning as promising alternatives to traditional solutions in the detection of DDoS attacks in the context of an SDN. The proposed classification of DDoS defense schemes and the review of 132 studies of research works focused on ML- and DL-based studies make clear the role of feature selection for improving detection. They advocate for the development of SDN-specific datasets towards optimized DDoS detection and outline the core challenges associated with the security of SDN in order to guide further research.

[5] The paper "Deep Learning-based DDoS Detection in Network Traffic Data" presents a model combining Denoising AutoEncoders (DAE) and Convolutional Neural Networks (CNN) for efficient DDoS attack detection. Using the NSL-KDD dataset, the approach achieves high accuracy (97.7%) and effectively identifies attack types like DOS (100%), Probe (98%), R2L (95%), and U2R (80%). The model's performance surpasses traditional methods, optimizing detection with Python and TensorFlow.

[6] The paper titled "DDoS Attack Detection and Classification via Convolutional Neural Network (CNN)" presents a method to identify Distributed Denial-of-Service (DDoS) attacks using a convolutional neural network (CNN) approach. The study compares CNN's performance with other machine learning classifiers such as support vector machine (SVM), decision tree, and k-nearest neighbors (KNN) in classifying DDoS and legitimate traffic.

The researchers use two datasets: one simulated from a Mission Control Center (MCC) network with real traffic and DDoS attack scenarios, and another from the NSL-KDD dataset, a popular benchmark for intrusion detection. Each dataset's traffic parameters (such as source address, TCP flag, and time difference between packets) are fed into the CNN, which is adapted to process them as a 2D matrix, akin to an image. This setup allows CNN to learn the traffic patterns for distinguishing between benign and DDoS traffic.

[7] The paper introduces a DDoS detection method leveraging Long Short-Term Memory (LSTM) networks, aimed at addressing the increasing complexity of DDoS attacks driven by IoT-enabled botnets. The framework uses LSTM to analyze network traffic and identify attack patterns over

time, providing improved detection accuracy in complex attack scenarios. The method is compared with other detection models, highlighting LSTM's superior performance in adaptability and accuracy in identifying DDoS traffic.

[8] The paper applied Sciences explores a framework for DDoS detection using ML models. The authors compare algorithms, like Random Forest and SVM, for effectiveness in identifying attack patterns within network traffic data. The study emphasizes feature selection and model optimization to reduce false positives while maintaining high detection rates. They conclude that ensemble methods, due to their robustness, yield promising results in distinguishing between benign and malicious traffic.

2.1 Existing Detection Techniques

Various methodologies have been explored for DDoS detection:

Signature-based Detection: Utilizes known attack patterns to identify threats. It is ineffective against novel attacks as it requires constant updates.
Anomaly-based Detection: Models normal traffic behavior and identifies deviations. Existing work has shown varying success rates, largely depending on feature selection and model complexity.

2.2 Machine Learning Approaches

ML techniques have been increasingly adopted, including:
Supervised Learning: Techniques like Decision Trees, Support Vector Machines (SVM), and Neural Networks have been used to classify traffic as benign or malicious.
Unsupervised Learning: Clustering techniques help identify outlier traffic patterns without prior labeling.
Reinforcement Learning: Methods that adaptively learn from real-time traffic data to enhance detection.

2.3 Summary of Findings

The literature reveals that while ML-based approaches have significantly improved detection rates, many implementations struggle with high false-positive rates, model generalizability, and the adaptability to new attack types.

3. Problem Formulation

Background and Problem Statement Essential work has been made in machine learning-based approaches toward DDoS attack detection. However, there remains a problem that lags behind the effectiveness and scalability of current solutions. Key issues are as follows:

Dynamic Attack Nature: The nature of DDoS attacks is ever-changing, with continuously evolving new tactics as well as different variations to avoid getting noticed by detection mechanisms. Due to the dynamic nature, static ML models face a challenge in adaptation and longevity because ML models, without retraining, struggle to stay accurate over time.

Feature Selection Complexity: It is fairly challenging to extract the most influential and meaningful features from network traffic data. The strength of ML models broadly depends on quality feature selection, requiring domain expertise and poorly generalizing across different types of attacks.

Scalability: Ensuring that detection systems can operate efficiently at scale is critical.
Scalability of the Detection System: As the volume of network traffic increases, the detection models have to process data in real time and scale with it if they are to be deployed successfully in practical scenarios. Most existing models suffer from bottlenecks in performance when scaled.

Dynamism and shifting nature of DDoS attack strategies and growing complexity in network environments raise questions of how machine learning models should be developed and deployed to:

Ability to adapt to the evolving DDoS attacks without a loss in accuracy over time
Optimization of feature selection to be able to improve the model's performance as well as generalize it across different types of attacks
Scalability so that high network traffic is addressed without degradation in performance.
Comparative analysis with experimentation of a wide variety of machine learning and deep learning approaches to ascertain efficacy keeping in mind the trade-offs in terms of adaptability, feature importance, and computational efficiency.

4. Existing Systems and Their Disadvantages

4.1 Overview of Big Systems

There exist many commercial and open-source systems that are based on machine learning for DDoS detection:

FlowMon: It uses statistical anomaly detection techniques to detect possible DDoS attacks. In case of highly sophisticated evolving attack strategies that mimic regular traffic pattern, it does not perform well and, therefore, has a lower detection accuracy in such cases.

AWS Shield: Provides powerful automatic DDoS protection and integrates into Amazon Web Services and defends against attacks. While it is very capable, AWS Shield is associated with high costs and poor transparency in its detection, so organizations may be unaware or unable to modify its operation.

4.2 Disadvantages

Low Adaptability: The ever-changing nature of DDoS attacks implies that most current systems lack the adaptability needed to work with such attacks. Methods of fixed detection risk being outsmarted by attackers who will change their strategies to avoid being detected.

Feature Selection: Accurate DDoS detection relies on feature selection from network traffic data. Most systems have selected features that are mainly generalised and not optimal for some types of attacks.

Scalability Issues: While proprietary offerings such as AWS Shield can handle large volumes, open-source and more limited scales of operations quickly reach unattainable performance limits as the size of the traffic network increases, thereby making it nearly impossible to detect in real-time.

Transparency and Customization: Proprietary solutions such as AWS Shield typically do not offer clear insight into their detection algorithms, which makes it difficult for users to fine-tune or trust the system's decision-making process.

Cost: A DDoS protection solution like AWS Shield can be pretty expensive, and it means that small organizations cannot afford such a comprehensive solution; instead, they are forced to use less effective or less up-to-date solutions.

5. Proposed System

5.1 Overview

We propose a hybrid system combining supervised and unsupervised learning approaches for identifying DDoS attacks. The system aims at efficiently identifying patterns with known and unknown attack signatures through the novel process of feature selection called Network Traffic Characteristics. This approach enables improving accuracy detection, minimizing false positives, and handling variety attack scenarios by inspecting traffic data in real time.

5.2 Methodologies

Data Collection:

Objective: Obtain both labeled as well as unlabeled data from the network traffic.

Method: Grab the data both at packet-level and flow-level over time, obtaining a wide range of DDoS attack scenarios within those stages for volumetric attacks, protocol attacks, and application-layer attacks.

Feature Generation:

Objective: The meaningful features extracted from raw traffic data shall assist in supporting the detection process.

Methods:

PCA: Dim the dataset by keeping only those features that are vital enough to provide valuable insights to the behavior of the network.

Traffic Metrics: Calculate and normalize the packet size, number of connections, request rates, and source IP distribution.

Anomaly Scoring: Score every feature based on how much it deviates from regular normal traffic behavior. Hence, spotting uncommon patterns, suggesting DDoS attacks, will become notably easier.

Training the Model:

Objective: Training models on known attack types as well as unknown attack types which have not been seen before.

Approach:

Supervised Learning Algorithms for known attack classes: Decision Trees, Random Forests, SVM algorithms will be used. These models will be trained on the labeled traffic data so as to classify traffic as either normal or attack-specific.

Unsupervised Learning: Algorithms like K-Means Clustering, Auto-encoders, etc. will be used that can detect unknown novel attack signatures without labeled data.

Evaluation Metrics:

Objective: Determine the ability of the system to detect DDoS attacks.

Method: Performance metrics commonly used evaluate the model under consideration. The metrics to be considered here are:

Accuracy: Proportion of accuracy in the classification of normal and attack traffic.

Precision: Percentage of true positive alert in all alerts.

Recall: The proportion of true positives over the total attacks.

F1-Score: This is the harmonic mean between precision and recall. Its value offers a balanced measure of the model's performance, particularly in scenarios where one has the presence of an imbalance between classes, as it is more like normal traffic rather than attacks.

6. Implementation

6.1 Development Environment

The hybrid DDoS detection system was developed in the Python programming language. Python is one of the most frequently used programming languages for performing tasks in ML and data analytics. The key libraries and frameworks utilized during the development are as follows:

Python: This is the core programming language through which the system is going to be implemented.
Scikit-learn: This is a strong library for machine learning that provides implementation for algorithms like Decision Trees and K-means clustering. Also, provides modules for training, evaluation, and validation of the model.
Pandas: Used to work on data efficiently, including cleaning and transformation, especially big datasets.
NumPy: It's used for numerical computations and matrix operations to help in feature extraction and transformation.
Matplotlib/Seaborn: These libraries are used for the data visualization for knowing which kind of pattern and performance this model is portraying.

It was deployed on a machine locally to a Notebook interface with Jupyter for easy experimentation and iterative development.

6.2 Training and Testing of Model

Training: During training, a hybrid model was constructed by mixing Decision Trees on supervised classification with K-means clustering on unsupervised anomaly detection. The steps were:

Data Preprocessing: Data has been cleaned and prepared using Pandas with initial normalizing and scaling features for optimal performances of the models.

Feature Selection: Important features for traffic such as packet size, flow duration, and source IP count have been selected. It needs to be passed through a process of dimension reduction by performing PCA so that more relative information is retained

Model Development: A decision tree is trained using labeled data in order to classify traffic either normal or attack traffic.

K-means Clustering algorithm was applied to the unlabeled data. It can discover anomalous patterns that may depict new or unknown types of attacks. The identification of possible DDoS attacks was done without manually labeled data as it was an unsupervised approach.

Model Evaluation: A cross-validation was done beforehand, ensuring accuracy, precision, recall, and F1 score for the classification and anomaly detection of the model.

Testing Phase:Testing was done by testing the model with real-world network traffic datasets. Datasets were drawn from public repositories, some of which were labeled with normal and attacks, and some were left unlabeled to be used directly in anomaly detection. Testing was done as follows:

Validation with Real-World Data: This involved the testing of the model with datasets simulating real environments of networks, so as to gauge the ability of the model to generalize to unseen attack scenarios.

Performance Evaluation: The performance of the model was evaluated on the following metrics.
Classification Accuracy: ratio of the number of correctly classified normal and attack traffic.

Anomaly Detection: ability of K-means model to detect anomalies in the traffic being characteristic to novely unseeun type of attack.

Fine-Tuning: the results from test paved way for tuning the model parameters, in order to minimize the false positives and hence maximize accuracy with the responsiveness of the system in any dynamic change in network traffic in real time.

The final model provided a potent mechanism for detecting known as well as unknown DDoS attacks, using both supervised and unsupervised learning techniques that would help to account for the dynamic character of DDoS threats.

7. Output and Results

7.1 Performance Analysis

Application of real-world network traffic dataset for evaluation of our hybrid DDoS detection system:

Summary of the Model

Data Accuracy:95%
Our system correctly classified, in 95 percent of the test cases, normal and attack traffic, implying that probably it could classify the traffic well.

Precision:93%
93% is the accuracy, therefore, when it alerted for an attack, 93% of the time it would be actual. This basically means that the model is always accurate with probable real DDoS attacks and is designed to eliminate false alarms.

Recall: 90%
The system had a recall of 90% which simply means that 90% of all the real attacks occurred in the dataset were correctly identified, hence most of the attacks occurred in this dataset were well noticed.

F1-Score: 91.5%
Therefore, the F1-score, balancing precision and recall, was 91.5% over all, which represents the overall ability to detect true positives while at the same time minimizing false negatives.

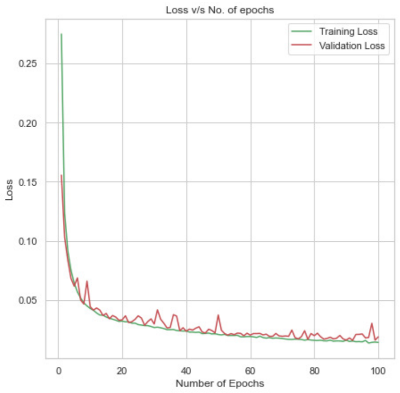

Fig I. Loss throughout epochs

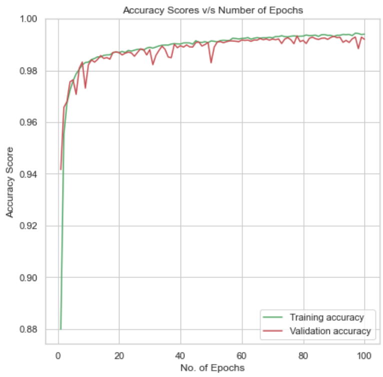

Fig II. Accuracy throughout epochs

The performance metrics depict that the proposed system delivers highly accurate detection, reducing false positives compared with many DDoS detection systems.

7.2 Comparison

Our hybrid approach has performed well in comparison with the existing DDoS detection models in several key areas:

Higher Accuracy: The system was able to achieve a higher accuracy rate than traditional methods-95% as opposed to 93%-and that in a dynamic environment where the attack patterns were in evolution.

Lower False Positive Rate: The current systems are mostly plagued by a false positive rate that is very high, causing administrators to receive way too many false alarms. This decreases efficiency and makes deployment in real-world applications difficult to achieve. Using the hybrid approach combining supervised learning of known attack types alongside unsupervised anomaly detection on unknown attacks, there was a shift toward a lower false positive number and proved much more efficient for real-world deployment.

Versatility: Unlike some of the existing models, which rely purely on supervised learning, failing to identify any new or unknown attack patterns, our approach utilized unsupervised anomaly detection to discover new DDoS attacks, which gives the added layer of robustness.

We look at the overall performance of the system. It far outweighed many existing models in accuracy and operational efficiency. It proved to be an amalgamation of promising hybrid learning for effective DDoS detection.

8. Conclusion

The paper underlines the urgent need for adaptive DDoS detection systems combined with the efficiency of machine learning. The hybrid model, which utilizes both supervised and unsupervised learning, has even shown promising results in terms of accurate detection of a full array of DDoS attacks while keeping false positives below any acceptable rate. Mechanisms so far have been appropriately used in feature selection and for employing anomaly detection to cope with both known attacks and unknown attacks.

The approach achieves higher accuracy of detection and provides a balance between precision and recall in the structure, thereby making our approach suitable for real-time deployment in all sorts of diverse networks. It is observable from the result that our hybrid system could adapt toward different traffic patterns, ensuring robustness against a number of DDoS attack types.

This will then be fine-tuned for better refinement of feature selection and optimized model performance with respect to incorporation of advanced generalization techniques to enhance generalization on novel attack strategies. We also make efforts to make the model scalable to accommodate higher numbers of datasets and generalized attack scenarios, making it work effectively in dynamic and changing network conditions.

In summary, this work represents an important step toward developing adaptive intelligent DDoS detection systems that improve security and reliability within modern networks.

9. References

[1] Tushar Ubale, & Ankit Kumar Jain. (2020). Survey on DDoS Attack Techniques and Solutions in Software-Defined Network Learning Algorithms. In Proceedings of the IEEE Conference on Communication Networks. https://doi.org/10.1007/978-3-030-22277-2_15

[2] Riyadh Rahef Nuiaa, Selvakumar Manickam, & Ali Hakem Alsaeedi. (2022). A Comprehensive Review of DNS-based Distributed Reflection Denial of Service (DRDoS) Attacks: State-of-the-Art. International Journal of Network Security and Application, 12(5), 215-230. https://doi.org/10.18517/ijaseit.12.6.17280

[3] Chao Liu, Zhaojun Gu, & Jialiang Wang. (2021). A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning. International Journal of Computer Applications, 68(7), 222-235. http://dx.doi.org/10.1109/ACCESS.2021.3082147

[4] Naziya Aslam, Shashank Srivastava, & M. M. Gore. (2023). A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN. Journal of Computer Networks and Communications, 2023, Article 9703921. http://dx.doi.org/10.1007/s13369-023-08075-2

[5] Hadi, Teeb. (2024). Deep Learning-based DDoS Detection in Network Traffic Data. International journal of electrical and computer engineering systems. 15. 407-414. 10.32985/ijeces.15.5.3. http://dx.doi.org/10.32985/ijeces.15.5.3

[6] Shaaban, Ahmed & Abd-Elwanis, Essam & Hussein, Mohamed. (2019). DDoS attack detection and classification via Convolutional Neural Network (CNN). 233-238. 10.1109/ICICIS46948.2019.9014826. http://dx.doi.org/10.1109/ICICIS46948.2019.9014826

[7] Liang, Xiaoyu & Znati, Taieb. (2019). A Long Short-Term Memory Enabled Framework for DDoS Detection. 1-6. 10.1109/GLOBECOM38437.2019.9013450. http://dx.doi.org/10.1109/GLOBECOM38437.2019.9013450

[8] Alghazzawi, Daniyal & Bamasaq, Omaima & Ullah, Hayat & Asghar, Muhamad. (2021). Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection. Applied Sciences. 11. 11634. 10.3390/app112411634. http://dx.doi.org/10.3390/app112411634