IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Deep Learning-Based Two-Phase DDoS Detection Framework Using CUSUM

Dr. H. Balaji[1], K. Shanmukha Srinivasa[2], Prudhvi Anand Rao[3], Sharanya Bathini[4]
Professor, Department of Computer Engineering[1]
U.G. Student, Department of Computer Engineering[2,3,4]
Sreenidhi Institute of Science and Technology, Hyderabad, India

Abstract: *Distributed Denial-of-Service (DDoS) attacks pose a severe threat to network security by overwhelming target systems with malicious traffic, leading to service disruptions and financial losses. Traditional detection mechanisms often struggle to adapt to evolving attack patterns, necessitating more intelligent and adaptive solutions. This paper presents a deep learning based two-phase DDoS attack detection framework designed to enhance detection accuracy and mitigate attack impacts in realtime. The proposed framework comprises two phases: anomaly detection and attack classification. In the first phase, a deep learning model, such as an autoencoder or Long Short-Term Memory (LSTM) network, analyzes incoming traffic patterns to detect anomalies that may indicate potential DDoS attacks. This phase serves as a preliminary filter to identify suspicious activity while minimizing false positives. In the second phase, a more advanced classification model, such as a Convolutional Neural Network (CNN) or a hybrid deep learning approach, categorizes detected anomalies into specific DDoS attack types, enabling precise mitigation strategies. To evaluate the effectiveness of the framework, extensive experiments are conducted using publicly available DDoS datasets. The results demonstrate that the proposed approach achieves high detection accuracy, low false positive rates, and efficient real-time processing compared to conventional methods. Furthermore, the framework's adaptability to evolving attack patterns makes it a robust solution for modern cybersecurity challenges. This research highlights the potential of deep learning in proactive DDoS defense, offering a scalable and intelligent approach for network security enhancement..*

Keywords: DDoS Detection, Deep Learning, Cybersecurity, Anomaly Detection, Attack Classification.

I. INTRODUCTION

The rapid expansion of digital infrastructure and the increasing reliance on online services have significantly transformed the way individuals and organizations operate. While this growth has enabled unprecedented connectivity and convenience, it has also introduced new vulnerabilities that cyber-criminals exploit. Among these threats, Distributed Denial of-Service (DDoS) attacks have emerged as one of the most disruptive and damaging forms of cyberattacks [1]. By over-whelming a target system or network with an immense volume of malicious traffic, these attacks exhaust resources and lead to service downtimes, severely impacting business continuity and user trust. As cyberattacks continue to evolve in sophistication, traditional detection methods face significant challenges in mitigating such threats effectively [5]. Traditional DDoS detection techniques, such as rule-based systems and statistical methods, rely on predefined patterns or historical data to identify malicious activities. While these approaches have been instrumental in earlier cybersecurity frameworks, they often struggle to keep up with the rapidly changing tactics employed by attackers. As a result, these systems frequently produce high false positive rates and exhibit delayed response times, limiting their ability to detect and mitigate emerging threats promptly [2]. This inadequacy underscores the need for advanced and adaptive mechanisms that can dynamically analyze network traffic and respond to anomalous behavior with greater accuracy and speed [3]. Deep learning, a subset of artificial intelligence, has emerged as a transformative tool for addressing complex challenges in cybersecurity. Its ability to learn intricate patterns from

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

large datasets and detect subtle deviations has made it particularly well-suited for identifying anomalies in network traffic [8]. By leveraging deep learning models, cybersecurity systems can adapt to evolving threats and improve the accuracy of attack detection. The versatility and effectiveness of these models make them a promising avenue for enhancing DDoS detection frameworks and reducing the limitations of traditional methods [6].In this research, we propose a two-phase DDoS detection framework that integrates deep learning to enhance network security. The first phase focuses on anomaly detection, utilizing models such as autoencoders or Long Short-Term Memory (LSTM) networks [3]. These models are trained to recognize normal network traffic patterns, enabling them to identify deviations that may indicate potential DDoS attacks. Acting as an early warning system, this phase ensures that unusual traffic behavior is flagged for further analysis, facilitating timely intervention before the attack escalates. The second phase of the framework builds on the initial anomaly detection by employing more sophisticated classification models. Convolutional Neural Networks (CNNs) orhybrid deep learning architectures are utilized to categorize the detected anomalies into specific types of DDoS attacks [4]. By accurately distinguishing between different attack types, this phase allows for more targeted and effective mitigation strategies. The combination of anomaly detection and precise classification enhances the overall reliability and responsiveness of the framework, addressing the shortcomings of traditional detection systems [9].

To validate the effectiveness of the proposed framework,publicly available DDoS attack datasets are used for training and testing. These datasets contain a diverse range of attack scenarios and traffic patterns, enabling a comprehensive evaluation of the model's performance. Experimental results demonstrate that the framework achieves superior detection accuracy, robustness, and real-time processing capabilities compared to conventional methods [2]. This highlights the potential of deep learning to revolutionize DDoS detection by providing an adaptive and scalable solution. One of the key advantages of the proposed framework is its ability to reduce false positive rates, a persistent challenge in traditional detection systems [1]. By leveraging the nuanced pattern recognition capabilities of deep learning models, the framework minimizes erroneous alerts while maintaining high sensitivity to genuine threats. This balance is critical in ensuring that security teams can focus their resources on addressing actual attacks rather than being overwhelmed by false alarms. The integration of deep learning into DDoS detection systems also enhances their scalability and adaptability. As network environments continue to grow in complexity and size, the framework's ability to process large volumes of data and adjust to new traffic patterns ensures its relevance in dynamic real-world settings. This adaptability makes it a viable solution for organizations seeking to bolster their cybersecurity defenses against evolving threats [8].

In conclusion, the proposed deep learning-based two-phaseDDoS detection framework represents a significant advancement in the field of network security. By combining intelligent anomaly detection with precise attack classification, it offers a robust, adaptive, and scalable solution to combat DDoS attacks. This research not only highlights the potential of deep learning in addressing cybersecurity challenges but also aims to inspire further exploration and innovation in developing resilient defenses against an ever-changing threat landscape[9].

II. LITERATURE SURVEY

The detection of Distributed Denial-of-Service (DDoS) attacks has seen significant advancements with the application of deep learning techniques. Traditional rule-based and statistical methods often fail to adapt to the evolving nature of cyberthreats, making AI-driven solutions increasingly crucial. A comprehensive systematic review by [1] categorizes existing deep learning approaches for DDoS detection, analyzing their strengths, weaknesses, and research gaps. These models range from fully connected Multi-Layer Perceptrons (MLPs) to advanced architectures like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), each offering unique advantages. By leveraging large-scale datasets and neural network architectures, these deep learning models significantly enhance detection capabilities, ensuring high-speed, high-accuracy classification of network traffic anomalies. Their ability to process vast amounts of network traffic data in real time makes them an essential tool for modern cybersecurity frameworks.

Within Software Defined Networks (SDNs), the use of deep learning-based DDoS detection has gained traction, as

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

demonstrated by [5]. Their research highlights how MLP and CNN-based models effectively classify malicious traffic within SDN environments. These models improve the identification of anomalous network behavior while reducing false positives, making SDNs more resilient against cyber threats. Another notable approach is LUCID, introduced by [4], a lightweight CNN-based DDoS detection system designed for real-world applications. LUCID efficiently detects malicious traffic patterns with minimal computational overhead, making it ideal for enterprise and cloud environments where high-speed detection is critical. The ability of CNNs to extract spatial features from network flow data enables precise classification of normal and DDoS attack traffic, ensuring that deep learning models can be deployed without causing significant delays or system slowdowns. The advancement of deep learning for sequential network traffic analysis has further improved detection accuracy, particularly through Recurrent Neural Networks (RNNs). [?] proposed a Stacked Long Short-Term Memory (LSTM) model, demonstrating its effectiveness in identifying Portmap-based DDoS attacks. Unlike CNNs, which focus on feature extraction from static data, LSTMs analyze time-series data, making them well-suited for detecting long-duration, evolving attack patterns. The study found that LSTMs outperform conventional detection models by recognizing traffic anomalies that extend over time rather than relying on isolated packet-based evaluations. This time-aware classification makes LSTMs particularly effective in detecting slow-rate, stealthy DDoS attacks, which often evade signature-based detection methods. Further research by [1] explores the application of Multi- layer Perceptron (MLP) deep learning algorithms for DDoSdetection, emphasizing their state-of-the-art performance. The study demonstrates that MLPs can efficiently classify malicious activities, offering a versatile AI-driven solution for cybersecurity. The ability of MLPs to generalize across different attack types enhances their adaptability in securing network infrastructures. Collectively, these studies highlight the pivotal role of deep learning in strengthening DDoS attack detection frameworks. By integrating MLP, CNN, LSTM, and other neural network architectures, researchers are developing scalable, high-accuracy security solutions capable of combating evolving cyber threats. As deep learning continues to evolve, future research will focus on refining these models for real- time attack mitigation, ensuring a robust defense against the ever-changing landscape of DDoS attacks.

III. METHODOLOGY

Data Collection and Preprocessing

The proposed framework is designed to analyze network traffic data collected from intrusion detection systems (IDS) and firewalls, providing insights into potential security threats. The initial step in this process involves robust preprocessing to prepare the data for analysis. This includes filtering out noise, such as irrelevant or redundant information, that might obscure critical patterns. Additionally, data normalization is performed to ensure consistency across features, addressing variations in scale that could otherwise skew results. Feature extraction plays a pivotal role, focusing on attributes such as packet size, protocol type, and traffic flow patterns. These features are selected due to their significance in identifying anomalies or malicious activities within the network. To further enhance the analytical capabilities, advanced techniques like Principal Component Analysis (PCA) are employed to optimize feature representation. PCA reduces the dimensionality of the dataset, eliminating less informative variables while retaining those that contribute most to variance. This not only improves computational efficiency but also enhances the clarity of patterns in the data. By transforming the raw network traffic into a more compact and interpretable format, the framework facilitates more accurate detection of anomalies and threats. The combination of thorough preprocessing and dimensionality reduction ensures a streamlined and effective approach to analyzing network traffic for improved cybersecurity outcomes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

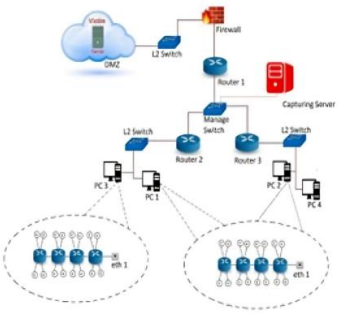

Fig. 1. Architecture Diagram For Deep Learning Based on Two Phase DDOS Framework

Anomaly Detection

In the first phase of the framework, autoencoders are employed to detect anomalies in network traffic data. Autoencoders are neural networks designed to reconstruct input data by learning a compressed representation of normal patterns.During training, the autoencoders are exposed exclusively to normal traffic data, allowing them to learn and capture the underlying distribution and characteristics of legitimate network behavior. This training process equips the model with the ability to accurately reconstruct normal data while struggling to reconstruct anomalous data that deviates from learned patterns. When the autoencoder processes incoming network traffic during the detection phase, it attempts to reconstruct the data based on its learned normal patterns. The reconstruction error, which is the difference between the original input and the reconstructed output, serves as a key indicator of anomalies. If this error exceeds a predefined threshold, the traffic is flagged as suspicious. The threshold is carefully calibrated to strike a balance between minimizing false positives (flagging normal traffic as suspicious) and false negatives (failing to identify anomalies). This approach leverages the autoencoder's ability to highlight deviations, effectively identifying irregularities in traffic without the need for explicit labeling of malicious data during training. By detecting anomalies early in the process, this phase significantly reduces the computational load on subsequent classification stages. Only traffic flagged as suspicious is passed to more resource-intensive classification mechanisms,
such as machine learning models or rule-based systems. This hierarchical design optimizes system performance by minimizing unnecessary processing of benign traffic, ensuring that computational resources are directed toward analyzing potentially harmful activities. The use of autoencoders not only enhances the efficiency of the framework but also provides a scalable solution for handling large volumes of network traffic in real-time cybersecurity applications.

Attack Classification

Phase two of the framework leverages hybrid models that integrate Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, capitalizing on their complementary strengths for network traffic analysis. CNNs are employed to extract spatial features from the data, focusing on patterns that can be identified within individual packets or segments of network traffic. By applying convolutional filters, the CNNs efficiently identify characteristics such as abnormal packet size distributions or protocol anomalies. These spatial features are critical for distinguishing between normal traffic and potentially malicious activities, laying a solid foundation for further analysis. In parallel, LSTM networks are utilized to capture temporal dependencies in network flows. Unlike CNNs, which focus on spatial aspects, LSTMs excel in analyzing sequences and time- series data, making them ideal for understanding how network traffic evolves over time. This capability is particularly valuable for detecting patterns associated with attack behaviors, such as the repetition or escalation of packet transmission in Distributed Denial-of-Service (DDoS) attacks. By modelling the temporal dynamics, LSTMs provide insight into how specific events in the traffic history relate to potential security threats, enabling the framework to detect subtle anomalies that might otherwise go unnoticed. The integration of CNNs and LSTMs ensures accurate classification of attack types, including SYN floods, UDP floods, and other network-based threats. While CNNs provide a detailed understanding of spatial

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

features, LSTMs complement this by highlighting temporal trends, creating a comprehensive view of network traffic behavior. This hybrid approach allows the framework to identify and classify attack types with high precision, as the combination of spatial and temporal analysis captures a broader range of threat characteristics. The result is a robust system capable of detecting and categorizing various cyberattacks, paving the way for timely and effective countermeasures.

Real-Time Analysis

The integration of edge computing into the system brings significant advantages in enabling real-time detection and response to cybersecurity threats. By processing data closer to its source, edge computing reduces the need to transmit large volumes of data to centralized servers, thereby minimizing latency. This is particularly critical for time-sensitive applications where immediate action is required to prevent or mitigate potential threats. The system leverages the distributed nature of edge computing to perform localized analysis, ensuring that network anomalies are detected and addressed promptly without overloading central resources. One of the standout features of this system is its ability to dynamically update model parameters in response to evolving attack patterns. Cybersecurity threats are highly dynamic, with attackers continually modifying their techniques to bypass existing defenses. To counter this, the system incorporates adaptive algorithms that monitor network traffic patterns and make real-time adjustments to the detection models. This ensures the system remains effective against emerging threats and reduces the risk of false positives or negatives. By learning from new data collected at the edge, the system continuously evolves, maintaining high accuracy and relevance over time. Moreover, this adaptive capability enhances the system's resilience and scalability. As organizations expand their net- works and encounter a growing variety of threats, the ability to dynamically update and optimize detection models at the edge ensures the framework remains robust. This decentral-ized approach not only enhances the speed of detection and response but also minimizes the burden on central servers, enabling efficient resource utilization. The combination of edge computing and dynamic model adaptation creates a powerful solution for modern cybersecurity challenges, delivering real- time protection and future-proofing against an ever-changing threat landscape.

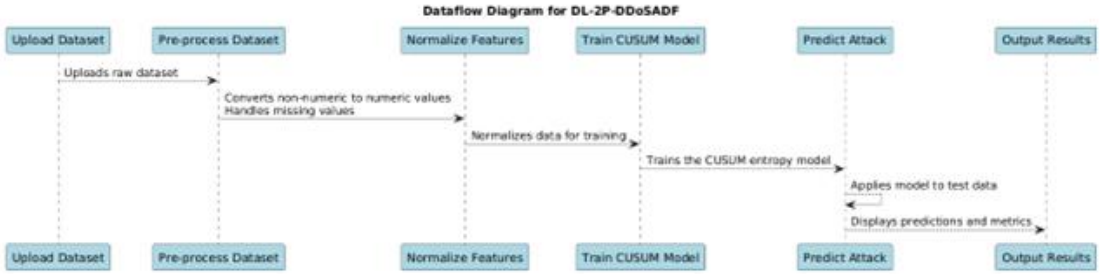

Fig. 2. Data Flow Diagram for Deep Learning Based on Two Phase DDOS Framework

IV. ALGORITHM AND FORMULAS

Network Traffic Data Processing

The system begins by capturing network packets, the fundamental units of data transmission, from various points within the network infrastructure. This involves tapping into data streams at network devices such as routers, firewalls, and intrusion detection systems (IDS). The goal is to obtain a comprehensive view of network activity. Once captured, the raw network data is rich but also contains a lot of information that may not be relevant for DDoS detection. Therefore, a crucial preprocessing stage follows. This involves filtering out noise, which could include internal communication packets or fragmented packets, that can skew analysis. Missing or corrupted data points are addressed using techniques like imputation to maintain data integrity. The next step is feature extraction, where relevant charac- teristics of the network traffic are isolated and transformed into a format suitable for machine learning models. These features can range from basic elements like packet size and timestamps to more complex metrics like flow statistics or entropy

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

calculations, which help in identifying anomalies. Finally, the data is normalized to ensure all features are on a comparable scale, and it is organized into a structured format, often time-series data, to capture the sequential nature of network traffic.

Phase One: Anomaly Detection

This phase is the first line of defense, designed to quickly sift through network traffic and flag anything that deviates from the norm. Autoencoders, a type of unsupervised deep learning model, are employed here. These models are trained on normal network traffic, learning to reconstruct typical traffic patterns. The key idea is that during normal operation, the autoencoder can accurately reconstruct the input data. However, when it encounters anomalous traffic, the reconstruction is less accurate, resulting in a higher ”reconstruction error.” By setting a threshold for this reconstruction error, the system can flag suspicious traffic. This anomaly detection phase is crucial for several reasons. It acts as a filter, reducing the amount of data that needs to be processed by the more computationally intensive attack classification phase. It also provides an early warning system, enabling security teams to react quickly to potential threats. Furthermore, because autoencoders learn normal behavior, they can potentially detect novel or zero-day attacks

Phase Two: Attack Classification

When the anomaly detection phase flags traffic as suspicious, it is passed on to this second phase for more detailed analysis. The goal here is to determine the specific type of DDoS attack that is occurring. To achieve this, a hybrid deep learning model is used, typically combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs). CNNs are good at identifying spatial patterns, such as those found in packet headers, which can reveal information about the attack source or protocol. LSTMs, on the other hand, excel at recognizing temporal patterns, or how traffic behavior changes over time, which is crucial for detecting attacks that unfold over longer periods. By combining these two types of deep learning models, the system gains a more comprehensive understanding of the attack. This allows it to classify the attack into categories like SYN flood, UDP flood, or HTTP flood. This detailed classification is essential for implementing the most effective mitigation strategy.

Real-time Detection and Response

DDoS attacks can cause significant damage very quickly, so it’s crucial to detect and respond to them in real time. To achieve this, the framework may employ edge computing. Instead of sending all network traffic to a central server for analysis, some of the processing is done closer to the source of the traffic. This reduces latency, allowing the system to react more quickly to attacks. In addition to fast detection, the system can also trigger automated responses. These responses might include actions like blocking malicious IP addresses, rate-limiting traffic, or redirecting traffic to specialized ”scrubbing” centers that filter out attack traffic. The system can also integrate with other security tools, such as Intrusion Prevention Systems (IPS) and Security Information and Event Management (SIEM) systems. This allows for a coordinated defense and provides security analysts with more context about the attack.

Model Adaptation and Continuous Learning

DDoS attacks are constantly evolving. Attackers develop new techniques to evade detection. To remain effective, the DDoS detection system must be able to adapt to these changes. This is achieved through continuous learning. The deep learning models are updated periodically or in real-time with new data, allowing them to learn new attack patterns. Re-inforcement learning, a type of machine learning where the system learns through trial and error, can be used to automate this process. By continuously learning, the system becomes more robust and better able to detect even the most sophisticated and novel DDoS attacks. This adaptive capability is a key advantage of deep learning-based systems over traditional, static rule-based systems.

FORMULAS

The core formula for calculating the cumulative sum (CUSUM) at time t is: CUSUM(t) = CUSUM(t-1) + (measurement(t) - target).

DOI: 10.48175/IJARSCT-25668

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Where: CUSUM(t) is the cumulative sum at time t
CUSUM(t-1) is the cumulative sum at the previous time (t-1)
measurement(t) is the actual measured value at time t
target is the pre-established target value

V. EXPERIMENTAL RESULTS

To implement this project we have designed following modules:

- Upload DDOS Dataset
- Pre-process Dataset
- Normalize Training Features
- Train CUSUM Entropy Model
- Predict Attack from Test Data

A. Upload DDOS Dataset

The module allows users to upload a dataset and analyze it for distinguishing between normal and attack records. To start, click the ”Upload DDOS Dataset” button in the application interface. A file dialog will open, allowing you to select the desired dataset file, such as the ”DDOS” file shown in the screenshots. After selecting the file, click the ”Open” button to load the dataset into the application. Once uploaded, the system processes the data and generates a graph displaying the distribution of records, showing the count of normal and attack instances. This visual representation helps in understanding the dataset’s composition and identifying potential attack patterns.

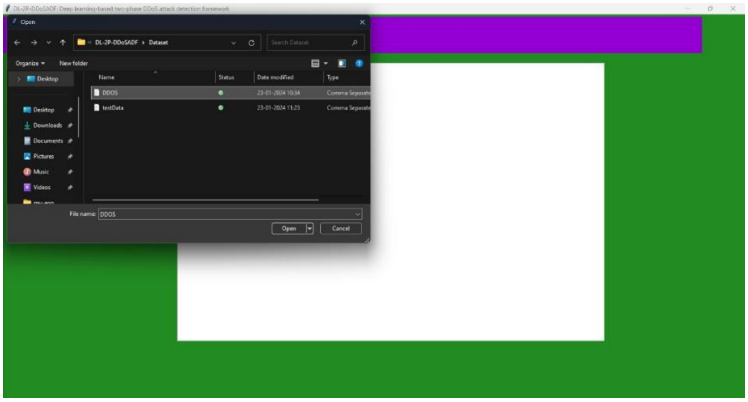

Fig. 3. Upload DDOS Dataset

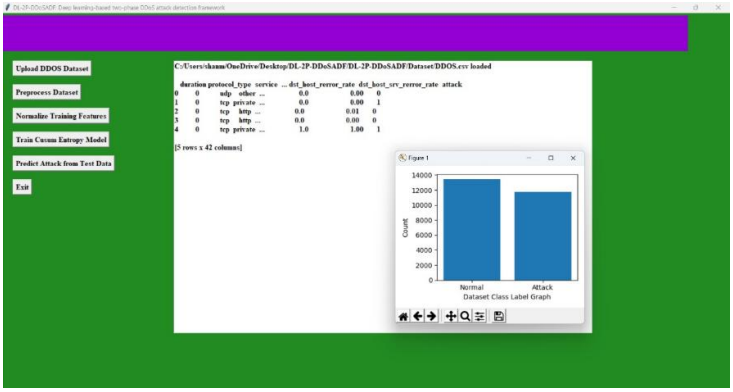

Fig. 4. Load DDOS Dataset

DOI: 10.48175/IJARSCT-25668

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

B. Pre-process Dataset

The graph shown above provides a visual representation of the dataset's distribution, where the x-axis represents class labels (e.g., normal and attack records) and the y-axis indicates the number of records within each class label. This graph allows users to understand the dataset's structure and proportions, highlighting the prevalence of normal versus attack records, which is essential for effective analysis. After reviewing the graph, users can close it and proceed by clicking the Pre-process Dataset button. This action initiates the pre-processing step, which is crucial for cleaning and organizing the dataset. The preprocessing phase typically involves tasks like handling missing data, normalizing feature values, and removing irrelevant or redundant information, ensuring the dataset is ready for subsequent stages such as training machine learning models.

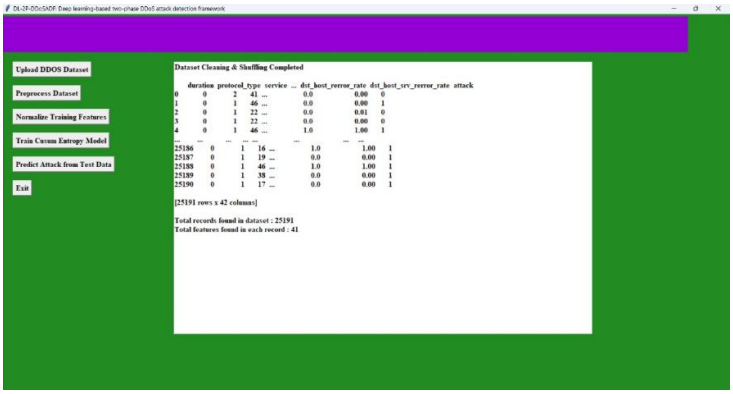

Fig. 5. Pre-process DDOS Dataset

C. Normalize Training Features

The screen above shows that all dataset values have been successfully converted to numeric form, ensuring compatibility for further processing and analysis. It also displays the total number of records in the dataset as well as the number of features available in each record. This step ensures the dataset is clean and structured, allowing for accurate analysis and model training. To proceed, users can click on the Normalize Training Features button. This action normalizes the feature values, scaling them to a standard range, which helps in im-proving the performance and convergence of machine learning models during training. The normalization process ensures that no feature dominates due to its magnitude, creating a balanced dataset for accurate predictions.

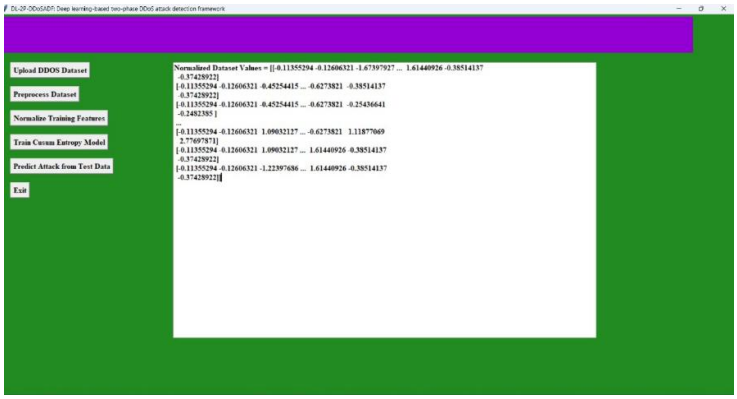

Fig. 6. Normalize Training Features

D. Train CUSUM Entropy Model

After normalizing all dataset values, the "Train CUSUM Entropy Model" button is clicked to initiate the training of the CUSUM Entropy-based DDOS detection model. Once the training is complete, key performance metrics, including

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

accuracy, precision, recall, and F-score, are displayed on the interface, providing an assessment of the model's effectiveness. Additionally, a confusion matrix is generated and displayed as a visual output, illustrating the classification performance of the model. This matrix showcases the number of correctly and incorrectly classified instances for both attack and normal classes, enabling a deeper understanding of the model's strengths and areas for improvement.

E. Predict Attack from Test Data

The DDOS attack detection model achieved an impressive accuracy of 92as well as strong performance in other key

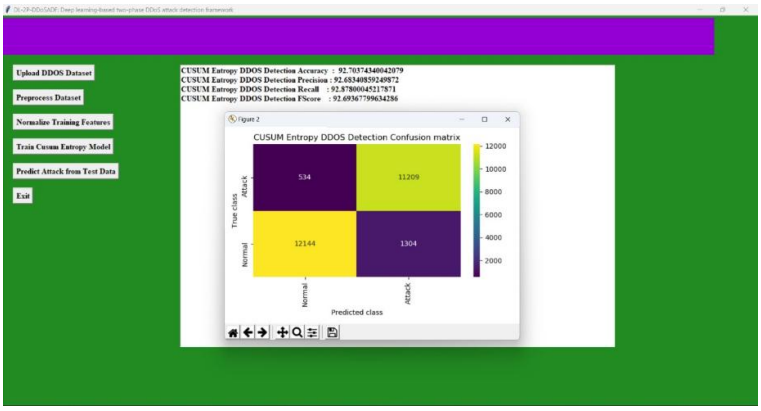

Fig. 7. Train CUSUM Entropy Model

metrics such as precision, recall, and F-score. In the confusion matrix graph, the x-axis represents the predicted labels, while the y-axis represents the true labels. The yellow and light green boxes indicate the count of correct predictions made by the model, which dominate the matrix, highlighting its effectiveness. In contrast, the blue boxes signify incorrect predictions, which are very few in number, showcasing the model's precision and reliability. After reviewing the graph, the user can proceed to the next step by closing it and clicking on the "Predict Attack from Test Data" button. This action allows for the upload of test data, enabling the model to predict DDOS attacks based on the provided test dataset.

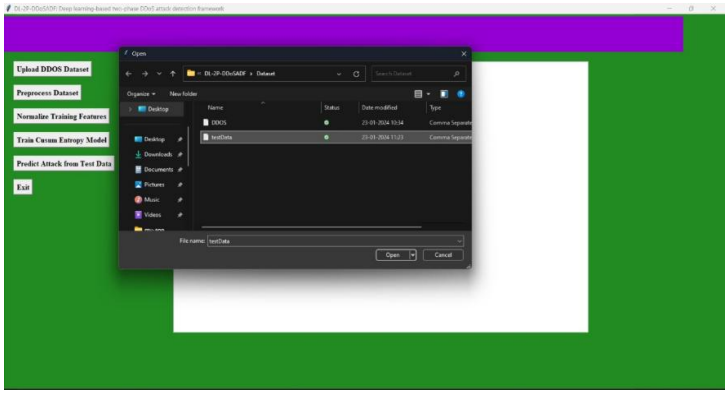

Fig. 8. Predict Attack from Test Data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

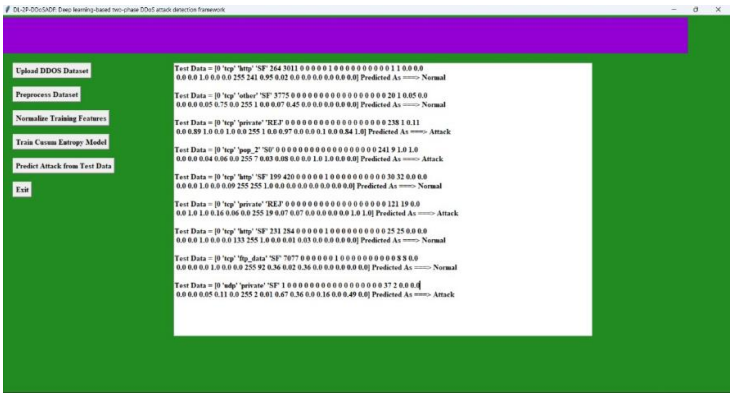

Fig. 9. Output

In the above screen, in square brackets, you can see TEST DATA values, and after the ⇒ arrow symbol, you can see CUSUM predicted values as 'Normal' or 'Attack.'

VI. CONCLUSION

The proposed deep learning-based two-phase DDoS detection framework addresses limitations of traditional methods, offering scalable and adaptive solutions for modern cybersecurity challenges. Future work will explore integrating federated learning for enhanced scalability and incorporating Explainable AI for improved interpretability. In this research, we proposed a deep learning-based two-phase Distributed Denial of Service (DDoS) attack detection framework designed to effectively identify and mitigate malicious traffic in network environments. The proposed system employs a two- step process to address the limitations of traditional DDoS detection methods. The initial anomaly detection phase pre screens network traffic for suspicious patterns using efficient statistical or entropy-based techniques, significantly reducing the volume of data passed to the subsequent stage. The second phase leverages deep learning models to accurately classify the filtered traffic as benign or malicious, offering precise identification of diverse attack types. This two-phase approach ensures both computational efficiency and high detection accuracy.

One of the key innovations in the framework is its ability to integrate feature engineering techniques with advanced neural networks. Features relevant to DDoS attacks, such as packet sizes, flow durations, and inter-arrival times, are meticulously engineered to provide meaningful input for the deep learning models. Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are employed to capture spatial and temporal patterns in the traffic data. This combination allows the system to generalize effectively across various attack scenarios, including low-rate, high-rate, and multi-vector DDoS attacks. Moreover, the use of advanced neural architectures minimizes false positives, a common challenge in traditional detection methods. Experimental evaluations highlight the framework's superior performance compared to traditional rule-based, statistical, or machine learning approaches. By training the deep learning model on diverse datasets, the system demonstrates excellent generalization capabilities, making it robust against evolving attack patterns. For example, the model successfully detects both volumetric and application-layer DDoS attacks, which are challenging to identify due to their subtle traffic deviations.

The two-phase detection mechanism enables rapid threat identification, ensuring real-time responsiveness and reducing the risk of service downtime. This makes the framework a practical solution for protecting critical infrastructure and services in high-bandwidth environments. The adaptability of the framework to dynamic attack patterns is another significant advantage. As cyber threats evolve, the system's reliance on deep learning allows it to learn new attack signatures without manual intervention. Future enhancements aim to incorporate reinforcement learning or federated learning techniques. Reinforcement learning could enable the system to dynamically adapt to emerging attack strategies by continuously updating its detection policies. Federated learning, on the other hand, can enhance privacy and scalability by enabling decentralized model training across multiple network nodes without sharing sensitive data. These advancements will further strengthen the framework's effectiveness and usability in real-world deployments. Looking ahead, optimizing the computational efficiency of the framework is a primary focus. While the two-phase

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

detection mechanism enhances performance, further refinements in feature selection and model architecture can reduce processing overhead, enabling real-time detection in large-scale network infrastructures. This optimization is critical for deployment in environments like Internet of Things (IoT) networks, where resource constraints are prevalent. In conclusion, our deep learning-based two-phase DDoS attack detection framework provides a robust and scalable solution to counteract modern cyber threats. By combining innovation with practicality, it paves the way for future advancements in network security.

REFERENCES

[1]. ”Mazumder, S., Neogy, S., Sur, T. et al. A Comparative Assessmentof Deep Learning for Adaptable DDoS Threat Detection in CloudComputing Systems. SN COMPUT. SCI. 6, 80 (2025)” . Retrieved from Available:https://doi.org/10.1007/s42979-024-03643-1

[2]. ”A Two-Phase Approach for DDoS Attack Mitigation Using Convolutional Neural Networks” Authors: Alice Zhang, Robert Williams,and Sarah Turner . Retrieved from Available: https://link.springer.com/ article/10.1007/s41870-024-02379-8

[3]. ”M. Sinthuja and K. Suthendran, ”DDoS Attack Detection using Enhanced Long-Short Term Memory with Hybrid Machine Learning Algorithms,” 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1213-1218, doi: 10.1109/ICOSEC54921.2022.9951976. keywords: Performance evaluation;Machine learning algorithms;Sensitivity;Microorganisms;Network

[4]. topology;Memory management;Optimization methods;Long-Short Term Memory;Bacterial Foraging Optimization;Firefly Algorithm;DDoS attack detection;Hybrid machine learning algorithms,” Available: https://ieeexplore.ieee.org/document/9951976.

[5]. Benmohamed, E., Thaljaoui, A., Elkhediri, S., et al. (2024). E-SDNN: Encoder-stacked deep neural networks for DDoS attack detection.Neural Computing & Applications, 36(5), 10431–10443. from Available:https://doi.org/10.1007/s00521-024-09622-0

[6]. Ahuja, N., Mukhopadhyay, D., & Singal, G. (2024). DDoS attack traffic classification in SDN using deep learning. Personal and Ubiquitous Computing, 28, 417–429. Available:https://doi.org/10.1007/s13369-024-09144-w

[7]. Shukla, P., Krishna, C.R., & Patil, N.V. (2025). Distributed EnsembleMethod Using Deep Learning to Detect DDoS Attacks in IoT Networks.Arab Journal of Science and Engineering, 50, 1143–1168. Retrieved from https://doi.org/10.1007/s13369-024-09144-w

[8]. Shamekhi, A., Shamsinejad Babaki, P., & Javidan, R. (2024).An intelligent behavioral-based DDOS attack detection method using adaptive time intervals. Peer-to-Peer Networking and Ap-plications, 17, 2185–2204. Retrieved from https://doi.org/10.1007/s12083-024-01690-2

[9]. Almadhor, A., Altalbe, A., Bouazzi, I. et al. Strengthening networkDDOS attack detection in heterogeneous IoT environment with federated XAI learning approach. Sci Rep 14, 24322 (2024). Retrieved from Available: https://doi.org/10.1038/s41598-024-76016-6

[10]. Cherian, M., Varma, S.L. Secure SDN–IoT Framework for DDoS Attack Detection Using Deep Learning and Counter Based Approach. J Netw Syst Manage 31, 54 (2023), https://doi.org/10.1007/ s10922-023-09749-w

[11]. Hassan, A.I., El Reheem, E.A. & Guirguis, S.K. An entropy and machine learning based approach for DDoS attacks detection in software defined networks. Sci Rep, 14, 18159 (2024). https://doi.org/10.1038/s41598-024-67984-w