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.



DOI: 10.48175/IJARSCT-25668