Abstract of the Thesis

Name: Dhangar Dharmeshkumar Natthuram

Enrollment No.: 219999913039

Faculty: CE/IT Engineering

Discipline/Branch: CE/IT Engineering

Title of the Thesis: "A Novel Mechanism to Fortify Application Layer against Distributed Denial of Service (DDoS) Attack"

Abstract

Distributed Denial-of-Service (DDoS) attacks remain a major cybersecurity challenge for enterprise networks, cloud platforms, and IoT environments. Traditional intrusion detection approaches often rely on static feature selection techniques, limiting their ability to identify evolving attack patterns and complex traffic behavior. To address this issue, this research proposes a Transformer-Based Attention CNN-BiLSTM framework for intelligent DDoS attack detection.

The proposed model combines a Transformer attention mechanism for dynamic feature weighting, CNN for spatial feature extraction, and BiLSTM for temporal dependency learning. This integrated architecture enables effective representation of network traffic characteristics and improves the distinction between benign and malicious flows.

The framework was evaluated on five benchmark datasets, namely CICDDoS2019, BCCC-cPacket-Cloud-DDoS-2024, CICIOT2023, ITDDoS2020, and APA-DDoS, covering enterprise, cloud, IoT, and advanced network environments. Experimental results demonstrate superior performance compared with conventional feature selection methods such as Mutual Information, ANOVA, and RFE. The proposed model achieved 98.74% accuracy, 98.70% F1-score, 0.9997 ROC-AUC, and 0.9842 MCC on CICDDoS2019, while cross-dataset validation produced accuracy ranging from 99.88% to 100%.

The results confirm that dynamic attention-based feature learning significantly enhances DDoS detection performance. The proposed framework demonstrates strong robustness, scalability, and generalization capability, making it a practical solution for real-time protection against modern DDoS attacks.

Keywords: DDoS Detection, Transformer Attention, CNN, BiLSTM, Deep Learning, Intrusion Detection System, Cybersecurity, Cloud Security, IoT Security.

This PhD Thesis will help in

OR

This Ph.D. Thesis would be useful for researchers, academicians, cybersecurity practitioners, network security analysts, cloud computing professionals, IoT security researchers, and organizations involved in designing intelligent intrusion detection and real-time DDoS defense systems.

List of Publication(s):

1. A Review of Defense Mechanisms against Distributed Denial-of-Service (DDoS) Attacks on the Application Layer, as well as Machine Learning (ML)-based Mechanisms to Defend Against DDoS Attacks, International Journal of Intelligent Systems and Applications in Engineering (IJISAE), Vol. 12, No. 21S, 2024 | ISSN: 2147-6799, SCOPUS Indexed Journal.
2. Adaptive Transformer-Gated Feature Selection With CNN–BiLSTM Hybrid Network for Efficient DDoS Attack Detection, International Journal of Advances in Signal and Image Sciences (IJASIS), Vol. 11, No. 6s, 2025 | Cite Score (2024): 11.6 (Q1), SCOPUS Indexed Journal.
3. TAFS-Net: A Transformer Attention-Based Feature Selection and BiLSTM Framework for Intelligent Cloud DDoS Attack Detection Using the BCCC-Packet-2024 Dataset, International Scientific Journal of Engineering and Management (ISJEM), ISSN: 2583-6129 | Impact Factor: 8.072.