Title: Effective Detection and Mitigation of DDoS Attacks Using Machine Learning and Deep Learning Techniques

Abstract: With the rapid expansion of internet technologies, cybersecurity threats such as Distributed Denial of Service (DDoS) attacks have become increasingly severe. These attacks overwhelm communication and computational resources, making detection and mitigation crucial. This study employs multiple machine learning and deep learning techniques, including K-Nearest Neighbors, Support Vector Machine, XGBoost, Decision Trees, Deep Neural Networks, and others, to detect DDoS attacks. The dataset used is SDN-specific and generated via a mininet emulator, containing both benign and malicious traffic data. Through extensive comparative analysis, models are evaluated based on accuracy and effectiveness in identifying malicious network activity. The results highlight the advantages of deep learning methods over traditional algorithms in terms of classification performance. To mitigate detected attacks, a simple rate-limiting technique is implemented to restrict abnormal traffic flow and prevent resource exhaustion. This study contributes to improving real-time DDoS detection and mitigation strategies, offering a robust approach to mitigating network security threats.

Introduction: DDoS attacks are a significant cybersecurity threat, capable of disrupting services and exhausting network resources. The increasing sophistication of these attacks necessitates advanced detection mechanisms that can differentiate between benign and malicious traffic.

Background and Previous Research: Prior studies have explored various intrusion detection systems, including rule-based and anomaly-based approaches, but traditional methods struggle with scalability and adaptability. Machine learning models have demonstrated promise in automating attack detection and reducing false positives in network traffic analysis.

Objectives: Existing solutions often lack real-time efficiency and robustness against evolving attack patterns. This study aims to develop a comparative evaluation of multiple machine learning and deep learning models to identify the most effective approach for DDoS detection and propose a simple mitigation technique.

Methodology: The study utilizes a dataset generated using a mininet emulator, simulating benign and malicious traffic, including TCP SYN, UDP flood, and ICMP attacks. Various machine learning models, including Decision Trees, Naïve Bayes, and Deep Neural Networks, are trained and evaluated based on accuracy and classification performance. Additionally, a rate-limiting technique is implemented to mitigate detected DDoS attacks by restricting abnormal traffic flow.

Expected Findings: It is anticipated that deep learning models, particularly Deep Neural Networks, will outperform traditional classifiers in terms of accuracy and real-time detection capabilities. Furthermore, the implementation of a simple rate-limiting technique is expected to reduce the impact of detected DDoS attacks, thereby enhancing network resilience.

Conclusion: This case study aims to enhance cybersecurity by identifying the most effective machine learning techniques for detecting and mitigating DDoS attacks, contributing to the development of robust network security frameworks.

Team :

Name	Roll Number
Anuvind M P	AM.EN.U4AIE22010
R S Harish Kumar	AM.EN.U4AIE22042
Girish S	AM.EN.U4AIE22044
Thazhai Mugunthan G	AM.EN.U4AIE22051