Chapter 13
Enhancing Security Measures Through Machine Learning Techniques for DDoS Attack Detection

S. Jayabharathi
https://orcid.org/0009-0008-3716-0936
SRM Institute of Science and Technology, Kattankulathur, India

B. Arthi
SRM Institute of Science and Technology, Kattankulathur, India

ABSTRACT

Distributed Denial of Service (DDoS) attacks have become an important threat to internet security with the hasty growth of the global digital population. These attacks aim to overwhelm target systems by flooding them with large network traffic, rendering them inaccessible to legitimate users. To address this challenge, this research paper proposes a machine learning-based approach for detecting and mitigating DDoS attacks. The study investigates the effectiveness of various machine learning techniques, including Long Short-Term Memory (LSTM), Support Vector Machines (SVM), and Logistic Regression, in accurately identifying DDoS attacks within network traffic. The outcomes demonstrate that the LSTM model attains the highest accuracy, with an accuracy score of 99.04%, outperforming traditional methods such as SVM and Logistic Regression. The proposed result leverages the unique capabilities of deep learning to capture complex patterns and long-term

DOI: 10.4018/979-8-3373-4672-4.ch013

INTRODUCTION

Global internet user growth has increased Distributed Denial of Service (DDoS) assaults, a danger to cybersecurity. There is a significant threat to the security of internet resources as the number of users grows. These attacks interfere with internet services and can seriously harm the economy, government, infrastructure, and business. Developing advanced techniques to identify and mitigate DDoS attacks is crucial to countering this evolving threat. Implementing machine learning algorithms to analyze and identify anomalies in network traffic patterns offers a promising approach for DDoS attack detection. These algorithms can significantly outperform existing detection techniques, making them powerful tools in the fight against DDoS attacks. Ongoing research and development are necessary to improve the effectiveness and reliability of machine learning algorithms across various information security applications, including detecting intelligent cybercrime such as DDoS attacks. This survey aims to provide a comprehensive overview of machine learning methods that can enhance the precision and capabilities of DDoS attack detection (Elsaeidy et al., 2019).

We examine several machine learning techniques that have shown promise in detecting DDoS attacks, including Support Vector Machine, Logistic Regression, K-Nearest Neighbor, Artificial Neural Network, and Random Forest. By leveraging these machine learning methods, researchers can enhance the accuracy and efficacy of DDoS attack detection, enabling proactive defenses against these online threats. Applying machine learning algorithms can significantly enhance the accuracy and effectiveness of DDoS attack detection, enabling proactive measures against online threats. Machine learning offers adaptable and self-learning systems, allowing them to detect and respond to evolving DDoS attack strategies in real time. Additionally, addressing the limitations of traditional rule-based methods requires exploring machine learning for DDoS attack detection. A more comprehensive and effective defense strategy can be achieved by leveraging machine learning to identify new and previously unseen types of DDoS attacks and adjust to changing attack patterns (Satyanarayana and Alasmi, 2022).

With the help of this research, it hopes to shed light on the state of machine learning-based DDoS attack detection today and emphasize the difficulties and potential associated with applying these methods to actual cybersecurity systems. It will examine the unique features of each machine learning method and how they are used to identify DDoS assaults in the sections that follow. Understanding what makes these algorithms exceptional will help us comprehend their potential impact on boosting cybersecurity defenses against DDoS attacks more fully. The many attacks that have been made using cloud computing technologies are identified in this survey article, along with the role that machine learning plays in establishing