ISSN: 2393-8048
International Conference of Education New Policy Relative to Computer
Venue: Sri Vinayak Mahavidhalya, Sri Vijaynagar, Rajasthan
23 May 2019

Machine Learning-Based Intrusion Detection for Modern Network Environments

Prerna Nagpal, Assistant Professor, Department of Computer Science, Sunrise University, Alwar

Abstract

The rapid growth of interconnected networks, cloud services, and Internet-based applications has significantly increased the risk of cyberattacks and unauthorized activities. Intrusion Detection Systems (IDS) play an important role in identifying malicious behavior and protecting network infrastructure from security threats. However, traditional signature-based intrusion detection techniques may have limited effectiveness against previously unknown attacks, evolving threat patterns, and large-scale network traffic. This paper presents a machine learning-based intrusion detection framework for identifying anomalous and malicious activities in modern network environments. The proposed approach analyzes network traffic and extracts relevant features such as packet characteristics, connection duration, protocol information, traffic volume, and behavioral patterns. Machine learning algorithms can then be trained to classify network activities as normal or potentially malicious. The framework can incorporate supervised learning techniques such as Random Forest, Support Vector Machine, and Gradient Boosting, along with appropriate preprocessing and feature-selection methods. The performance of the proposed system can be evaluated using publicly available intrusion detection datasets and standard metrics, including accuracy, precision, recall, F1-score, and false-positive rate. A comparative analysis of different machine learning models can further identify their effectiveness under varying network conditions. The proposed approach aims to improve the adaptability and detection capability of IDS while reducing false alarms. The study also discusses challenges such as imbalanced datasets, high-dimensional network features, real-time processing requirements, and the detection of previously unseen attacks.

Keywords: Machine Learning, Intrusion Detection System, Network Security, Cybersecurity, Anomaly Detection, Network Traffic, Classification, Feature Selection, Cyber Attacks