IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Anomaly Detection in Network Traffic Using Unsupervised Machine Learning

Dipali Paradhi, Mehjabeen Naghma Ansari, Sharmila More
MIT Arts, Commerce and Science College, Alandi, Pune, Maharashtra, India

Abstract: *With the increasing complexity and volume of network traffic, the detection of anomalies has become crucial for maintaining the security and efficiency of computer networks. Traditional rule-based methods often struggle to keep pace with the evolving nature of Cyber threats. In this paper, we propose utilizing unsupervised machine learning techniques for anomaly detection in network traffic. We explore various algorithms including k-means clustering, Isolation Forest, and auto encoders to identify abnormal patterns within network data without the need for labeled examples. Our experiments demonstrate the effectiveness of these approaches in detecting anomalies accurately and efficiently. Furthermore, we discuss the challenges and opportunities in deploying unsupervised machine learning for network anomaly detection in real-world scenarios. This research contributes to the advancement of Cyber security by providing novel methodologies for detecting suspicious activities within network traffic data, thereby enhancing the resilience of computer networks against emerging threats. Unsupervised methods, such as clustering algorithms like k-means or density-based techniques like DB-SCAN, can detect deviations from normal patterns in network traffic, indicating potential intrusions or anomalies. These systems analyze various features of network traffic, such as packet headers, traffic volume, and protocol behavior, to identify suspicious activity. However, they may also generate false positives and require careful tuning to balance detection accuracy and performance.*

Keywords: Cyber threats