EAI Endorsed Transactions
on Industrial Network and Intelligent Systems
Research Article EAI.EU

# Machine Learning in Cybersecurity: Advanced Detection and Classification Techniques for Network Traffic Environments

Samer El Hajj Hassan [1*], Nghia Duong-Trung[2,3]

[1] IU International University of Applied Sciences, Berlin campus, Frankfurter Allee 73A, 10247 Berlin, Germany
[2] German Research Centre for Artificial Intelligence (DFKI), Alt-Moabit 91 C,10559 Berlin, Germany
[3] Kien Giang University, 320 A - Highway 61 - Minh Luong Town, Chau Thanh District - Kien Giang Province, Vietnam

## Abstract

In the digital age, the integrity of business operations and the smoothness of their execution heavily depend on cybersecurity and network efficiency. The need for robust solutions to prevent cyber threats and enhance network functionality has never been more critical. This research aims to utilize machine learning (ML) techniques for the meticulous analysis of network traffic, with the dual goals of detecting anomalies and categorizing network activities to bolster security and performance. Employing a detailed methodology, this study begins with data preparation and progresses through to the deployment of advanced ML models, including logistic regression, decision trees, and ensemble learning techniques. This approach ensures the accuracy of the analysis and facilitates a nuanced understanding of network dynamics. Our findings indicate a notable enhancement in identifying network inefficiencies and in the more accurate classification of network traffic. The application of ML models significantly reduces network delays and bottlenecks by providing a strong defence strategy against cyber threats and network shortcomings, thereby improving user satisfaction, and boosting the organizational reputation as a secure and effective service layer.
Conclusively, the research highlights the pivotal role of machine learning in network traffic analysis, offering innovative insights and fresh perspectives on anomaly detection and the identification of malicious activities. It lays a foundation for future explorations and acts as an evaluation benchmark in the fields of cybersecurity and network management.

**Keywords:** Machine Learning, Cybersecurity, Network Analysis, Anomaly Detection, Data Security, Traffic Classification, Network Optimization, Traffic Volume

Received on 29 February 2024, accepted on 05 May 2024, published on 01 July 2024

Copyright © 2024 S. El Hajj Hassan *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetinis.v11i3.5237

*Corresponding author. Email: samer.elhajjhassan@iu-study.org

## 1. Introduction

In the rapidly evolving digital landscape, cybersecurity has emerged as a critical concern for businesses and organizations worldwide [1][2]. Cybersecurity and network performance are pivotal elements in maintaining the integrity and efficiency of technological infrastructures [3][4]. The world we live in is increasingly interconnected, with vast amounts of data being transferred every second across networks. This scenario presents both opportunities and challenges, especially in the realms of data protection and network optimization. Network issues affect customer satisfaction and company reputation significantly [3]. Users demand fast, secure access to services; delays or

*Corresponding author: Samer El Hajj Hassan
Email: samerhajjhassan@gmail.com