Network Anomaly detection using Machine Learning

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfilment of the Requirements for the Bachelor's degree in Information Security of Information Technology.

by

Kawther Haitham Kadhim Ghalib

Supervised by

Assist. Lec. Hassan Abdulameer

2023-2024

ABSTRACT

Network anomaly detection using machine learning is a technique that has gained significant attention in recent years due to the increasing frequency and complexity of network attacks. This approach aims to use machine learning algorithms to analyze network traffic and identify any anomalous behavior that may indicate a security breach or potential threat. In this paper, we present an overview of the current state of research on network anomaly detection using machine learning. We describe the various machine learning algorithms that have been applied to this problem, including unsupervised, supervised, and semi-supervised techniques.

We also discuss the challenges and limitations of using machine learning for network anomaly detection, such as the need for large datasets, the difficulty of interpreting results, and the potential for false positives and false negatives. Finally, we conclude by highlighting the importance of continued research in this area to improve the accuracy and effectiveness of network security measures.