A Machine Learning-Based Intrusion Detection System for Android Network Security Using Random Forest and Neural Networks

Abdulrazag Mustafa Alaswad
Libyan Center for Electronic Systems, Programming and Aviation Research, Tripoli, Libya

Haitham Saleh Ben Abdelmula
Libyan Center for Electronic Systems, Programming and Aviation Research, Tripoli, Libya

Akram Mohammed Imbarak
Libyan Center for Electronic Systems, Programming and Aviation Research, Tripoli, Libya

Abstract:
The rapid growth of Android devices and cloud-connected applications has significantly increased exposure to cyber threats and network-based attacks. Traditional Intrusion Detection Systems (IDS) often struggle to identify modern and evolving attack patterns due to the increasing complexity and volume of network traffic. This paper presents a machine learning-based intrusion detection framework utilizing Random Forest and Multi-Layer Perceptron (MLP) models. The proposed system is evaluated using the CICIDS2017 and UNSW-NB15 benchmark datasets. Experimental results demonstrate high detection accuracy and strong performance in distinguishing between benign and malicious traffic, achieving an overall classification accuracy of 93%. Among the evaluated malware categories, the model achieved the best performance in detecting Android SMS Malware, with a precision of 0.98, recall of 0.96, and F1-score of 0.97, indicating a strong ability to accurately identify malicious behavior while maintaining a low false positive rate. In addition, visualization techniques, including feature importance analysis and confusion matrices, are employed to improve model interpretability. The findings highlight the effectiveness of machine learning approaches for real-time intrusion detection, Android malware detection, and network-based intrusion analysis.

Keywords:
Intrusion Detection System, Machine Learning, Random Forest, Neural Networks, Cybersecurity, CICIDS2017, UNSW-NB15.