

Machine Learning for Cybersecurity in Malware Detection

Rajat Dahiya

M.Tech, Department of CSE,

Sat Kabir Institute of Technology and Management, Bahadurgarh, India

Abstract: *The rise of sophisticated malware poses a significant threat to cybersecurity, necessitating advanced detection methods beyond traditional techniques. This paper investigates the application of machine learning (ML) for enhancing malware detection capabilities. We review various ML algorithms, such as decision trees, support vector machines, and neural networks, highlighting their effectiveness in identifying and classifying malware. Our study utilizes multiple datasets, including public malware repositories, to train and evaluate these models. The results demonstrate that ML-based approaches significantly improve detection accuracy, precision, and recall compared to conventional methods. Furthermore, we discuss the challenges associated with ML in cybersecurity, such as adversarial attacks and the need for large, diverse datasets. Our findings underscore the potential of ML to provide robust defenses against evolving malware threats, offering insights into future research directions for bolstering cybersecurity frameworks.*

Keywords: Machine Learning, Cybersecurity, Malware Detection, Neural Networks, Random Forests, Support Vector Machines, Gradient Boosting Machines