IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, October 2025
Impact Factor: 7.67

AI Threat Detection Malware Analysis

Siddhant Mundre[1], Prof. D. G. Ingale[2], Prof. A. P. Jadhao[3], Prof. S. V. Raut[4], Prof. R. N. Solanke[5]
Student, CSE, Dr. Rajendra Gode Institute of Technology and Research, Amravati, India[1]
Guide, CSE, Dr. Rajendra Gode Institute of Technology and Research, Amravati, India[2]
Mentor, CSE, Dr. Rajendra Gode Institute of Technology and Research, Amravati, India[3,4,5]

Abstract: *This paper examines the application of artificial intelligence (AI) and machine learning (ML) techniques for threat detection and malicious software (malware) analysis. As cyber threats escalate in volume and sophistication, conventional signature-driven defences struggle against polymorphic and zero-day attacks. AI-powered methods — spanning static, dynamic and hybrid analysis — bring adaptability, pattern recognition, and automation to cybersecurity operations. The manuscript surveys contemporary literature, evaluates prevailing approaches, identifies limitations such as adversarial evasion and dataset bias, and proposes a hybrid framework combining static feature extraction, behavioural dynamic analysis, and an adversarially-hardened ensemble of deep learning and interpretable models. Empirical guidance for dataset curation, evaluation metrics, and deployment considerations is offered. The paper concludes with prospective directions including threat-intelligence integration, federated learning for privacy-preserving detection, and model explainability to enhance forensic utility. This research aims to furnish practitioners and researchers with a consolidated yet practical reference for advancing AI-driven malware defences*

Keywords: Artificial Intelligence; Machine Learning; Malware Analysis; Threat Detection; Deep Learning; Static Analysis; Dynamic Analysis; Adversarial Robustness; Explainable AI; Intrusion Detection

DOI: 10.48175/IJARSCT-29191