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 3, Issue 1, December 2023
Impact Factor: 7.301

A Systematic Review of Machine Learning and Deep Learning Approaches for Malware Detection in Cloud Computing Environments: Taxonomy, Architectures, and Open Challenges

[1*]Sanaboyina. Madhusudhana Rao, [2*]Arpit Jain
[1*,2*]Department of Computer Science and Engineering,
[1*,2*]Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, Andhra Pradesh, India.
[1*]smadhusudhan780@gmail.com[2*]drjainarpit@gmail.com

Abstract: *Cloud computing has become the backbone of modern digital infrastructure, hosting data, applications, and services for enterprises, governments, and individuals at unprecedented scale. This same concentration of computational and informational value, however, makes cloud platforms a high-priority target for malware authors, whose techniques now include polymorphism, metamorphism, fileless execution, multi-stage payload delivery, and adversarial evasion of learning-based detectors. Traditional signature-driven antivirus engines, designed for a single endpoint, cannot keep pace with the volume, velocity, and variety of malware encountered in multi-tenant virtualized and containerized environments. This paper presents a systematic review of machine learning (ML) and deep learning (DL) approaches for malware analysis and detection in cloud computing environments. We synthesize the literature into a unified taxonomy spanning analysis paradigms (static, dynamic, hybrid, and memory-introspection-based), feature representations (opcode and byte sequences, application programming interface and system-call traces, network telemetry, resource-utilization signals, and image-based encodings), and learning models (classical classifiers, deep neural architectures, ensembles, and federated learning). We further organize cloud-specific detection architectures into client-server scanning, hypervisor-level virtual machine introspection, container and orchestration monitoring, and edge-cloud collaborative pipelines. A comparative analysis of representative studies is provided, alongside a consolidated review of public datasets and evaluation metrics. Building on the gaps identified, we propose a layered conceptual framework for scalable, privacy-preserving, and explainable malware detection that operates at both the virtual-machine and service levels. Finally, we discuss persistent challenges—concept drift, class imbalance, adversarial robustness, non-deterministic replay, interoperability, and the resource overhead of detection—and outline future research directions, including self-healing detection, continual learning, and the integration of large language models for behavioral reasoning. This review is intended to help researchers position new contributions and to inform the design of next-generation, high-quality-of-service malware detection systems for the cloud.*

Keywords: *malware detection, cloud computing, machine learning, deep learning, virtual machine introspection, intrusion detection, container security, adversarial robustness, feature engineering, cyber-physical systems*