A3

From Network Flows to Memory Dumps: Advancing Hybrid Deep Learning for Fileless Malware Detection

Ayesha Ajmal (PhD) Faculty of Design & Creative Technologies

Fileless malware has emerged as one of the most evasive and technically sophisticated threats in cybersecurity. Unlike traditional malware, these attacks operate entirely within a system's volatile memory and exploit legitimate utilities such as PowerShell and Windows Management Instrumentation (WMI) while leaving no traces on permanent storage. Consequently, signature-based detection techniques are often ineffective against these attacks. This paper presents a systematic literature review of hybrid deep learning approaches for fileless malware detection published between 2020 and 2025 and, building on the gaps identified, proposes a novel hybrid deep learning framework for memory-based and network-based analysis.

In-depth analysis of research published between 2020 and 2025 highlights several key limitations that hinder progress in this field. Hybrid architectures combining Convolutional Neural Network (CNN)-autoencoders with transformer-based pipelines demonstrate strong detection accuracy by learning behavioural patterns from memory dumps and network flows (Demmese et al., 2023). However, these results are limited by small, outdated, and insufficiently representative datasets. Many datasets rely on file-based labels and do not adequately capture the memory-resident execution behaviour of fileless malware. The literature further identifies seven recurring methodological themes, including inconsistencies in data sources, feature selection strategies, and evaluation metrics, making cross-study comparison unreliable (Farhan et al., 2025).

Building on these findings, this review proposes a hybrid deep learning framework to be developed using a Design Science Research (DSR) methodology integrated with a Design-Oriented Machine Learning approach. The framework builds on standardised multi-metric evaluation protocols that move beyond accuracy (Ali et al., 2025); extending them with two novel contributions: a holistic feature extraction mechanism capturing fileless malware behaviour within network packet capture (PCAP) files, and a hybrid deep learning model optimised for memory-resident threat detection. Unlike Farhan et al. (2025) and Ali et al. (2025), whose work addresses network intrusion detection broadly, this research applies and extends these methodological and evaluation standards specifically to the fileless malware domain, combining memory and network-based analysis within a single hybrid deep learning framework. The work ultimately argues that progress in this field is limited not by insufficient modelling techniques, but by the lack of dedicated large-scale datasets for fileless attacks and unified benchmarks for evaluation.

Keywords
fileless malware, hybrid deep-learning, network intrusion detection, systematic literature review, memory forensics

References

Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences*, *15*(4), 1903. https://doi.org/10.3390/app15041903

Demmese, F. A., Neupane, A., Khorsandroo, S., Wang, M., Roy, K., & Fu, Y. (2023). Machine learning based fileless malware traffic classification using image visualization. *Cybersecurity*, *6*(1), 32. https://doi.org/10.1186/s42400-023-00170-z

Farhan, M., Waheed Ud Din, H., Ullah, S., Hussain, M. S., Khan, M. A., Mazhar, T., Khattak, U. F., & Jaghdam, I. H. (2025). Network-based intrusion detection using deep learning technique. *Scientific Reports*, *15*(1), 25550. https://doi.org/10.1038/s41598-025-08770-0