ISCSITR - International Journal of Cyber Security (ISCSITR-IJCS)
Vol.1, Iss. 1, January - March, 2025, pp. 19-25.
ISSN: XXXX-XXXX

Research Article

Dynamic Malware Analysis Using AI-Powered Binary Classification and Automated Reverse Engineering

Stavros A. V,
Penetration Tester,
Canada

Abstract

The rise of sophisticated malware has rendered traditional detection mechanisms increasingly ineffective. This research investigates how dynamic malware analysis, augmented by artificial intelligence (AI)-powered binary classification and automated reverse engineering, can bolster cybersecurity frameworks. The paper explores dynamic behavioral inspection integrated with deep learning models to improve malware classification accuracy. By leveraging reverse engineering automation, the proposed methodology enhances malware de-obfuscation and family attribution. Experimental results using real-world malware datasets demonstrate detection accuracies exceeding 95%, significantly reducing manual analysis time. This paper contributes to advancing proactive malware defense through hybrid AI and automation-based solutions.

Keywords:

Dynamic Analysis, Malware Detection, AI-Powered Classification, Reverse Engineering, Deep Learning, Binary Analysis, Cybersecurity, Threat Intelligence.

Citation: Stavros, A.V. (2025). Dynamic Malware Analysis Using AI-Powered Binary Classification and Automated Reverse Engineering. ISCSITR - International Journal of Cyber Security (ISCSITR-IJCS), 1(1), 19–25.

1. Introduction

Malware continues to evolve with enhanced stealth and polymorphism, posing a persistent threat to global cybersecurity. Traditional signature-based detection systems fall short when addressing zero-day attacks or novel variants. In response, dynamic malware analysis—a method that observes malware behavior during execution—has gained traction. Yet, this approach is resource-intensive and requires significant manual effort. To address these challenges, this study introduces an AI-driven methodology that combines binary classification and automated reverse engineering to accelerate malware identification and analysis.

AI-powered dynamic analysis empowers detection mechanisms to learn from behavioral features such as system calls, network activity, and file operations. Binary classification models categorize malware as either benign or malicious based on these behavioral traits. Meanwhile, reverse engineering tools like IDA Pro or Ghidra automate the process of disassembling and analyzing executable code. When these two methodologies are combined, they provide a powerful framework for real-time malware detection and threat intelligence. This paper discusses the underlying techniques, evaluates model performance on benchmark datasets, and provides recommendations for operational deployment.

2. Literature Review

Several studies have proposed hybrid solutions integrating machine learning with reverse engineering for improved malware detection.

- **Gaber et al. (2023)** provided a systematic literature review of AI-powered malware detection and outlined how dynamic analysis can reveal evasive malware behaviors that static analysis often misses. They emphasized using deep learning models like CNNs and RNNs for behavioral pattern recognition.
- **Poudyal & Dasgupta (2021)** built a multi-level profiling system incorporating AI based analysis for crypto-ransomware using both static and dynamic features, showing enhanced detection rates compared to standalone techniques.
- **Al Balawi et al. (2024)** demonstrated the use of Generative AI models in detecting malware by reverse engineering behaviors and patterns extracted from runtime executions.
- **Farzaan et al. (2024)** introduced an AI-enabled system in cloud security for dynamic analysis and incident response, reinforcing the role of real-time reverse engineering for attack mitigation.
- **Lumpatki & Patwardhan (2024)** emphasized binary-level reverse engineering combined with AI for malware family classification and anomaly detection.

- **Jasim (2024)** conducted a review on Android malware detection where binary classification models trained on dynamic traces outperformed traditional models by 20%.
- **Gebrehans et al. (2025)** presented a GAN-based approach for dynamic malware behavior simulation, proposing a multi-class classifier beyond traditional binary models.
- **Tyagi & Addula (2024)** analyzed disassembly tools and proposed combining static and dynamic results for improved automated reverse engineering.

3. Methodology

This study adopts a hybrid model consisting of:

- **Dynamic Feature Extraction**: Using sandboxing tools (e.g., Cuckoo) to record real time system interactions.
- **Binary Classification**: Implementing Random Forests and Deep Neural Networks to classify files.
- **Automated Reverse Engineering**: Utilizing IDA Pro and Ghidra to decompile and extract low-level binary logic.

A labeled dataset of 20,000 samples from VirusShare was used. The training-test split was 80:20.

3.1 Dynamic Feature Extraction

Dynamic feature extraction is the process of observing how a suspicious file behaves when it is executed in a controlled environment. This approach is crucial for detecting evasive malware that may alter behavior when it detects static analysis or virtualization.

- Sandboxing Tools (e.g., Cuckoo Sandbox): These are secure environments where malware can be executed without harming the host system.

- Captured Behaviors Include: System calls, registry modifications, network connections, file system changes, process spawning, and API usage.
- Purpose: These behaviors are converted into structured data (features) that can be used to train machine learning models.

3.2 Binary Classification

Binary classification is a machine learning technique where the goal is to categorize inputs into one of two classes: **malicious** or **benign**.

- **Random Forest:** A classical ensemble method that uses multiple decision trees to make predictions. It's known for robustness and interpretability.
- **Deep Neural Networks (DNNs):** A more advanced approach using layered neural architectures. DNNs can automatically learn complex feature representations, making them suitable for identifying subtle malicious patterns.
- **Input:** Behavioral features extracted from dynamic analysis.
- **Output:** A prediction label “malware” or “not malware.”

3.3 Automated Reverse Engineering

Reverse engineering is the practice of analyzing a program’s binary code to understand its structure and behavior—particularly useful when source code is unavailable.

- **IDA Pro & Ghidra:** Industry-standard reverse engineering tools that decompile executable files into assembly code or higher-level representations.
- **Automation:** Instead of manual inspection (which is slow and requires expertise), scripts and AI plugins can automate parts of the analysis—such as identifying function calls, control flows, or encryption routines.
- **Use Case in Malware Analysis:** Helps reveal hidden payloads, unpack encrypted code, or understand how malware communicates with its command-and-control server.

Table 1: Dataset Summary

Dataset	Samples	Malware	Benign	Source
VirusShare	20,000	10,000	10,000	virusshare.com
Custom Sandboxed	5,000	2,800	2,200	In-house logs

4. Results and Discussion

Two models were tested: Random Forest and DNN. The DNN achieved **95.7% accuracy**, outperforming Random Forest's **91.2%**. Reverse engineering enabled deeper insights into malware functionalities such as keylogging and ransomware payloads.

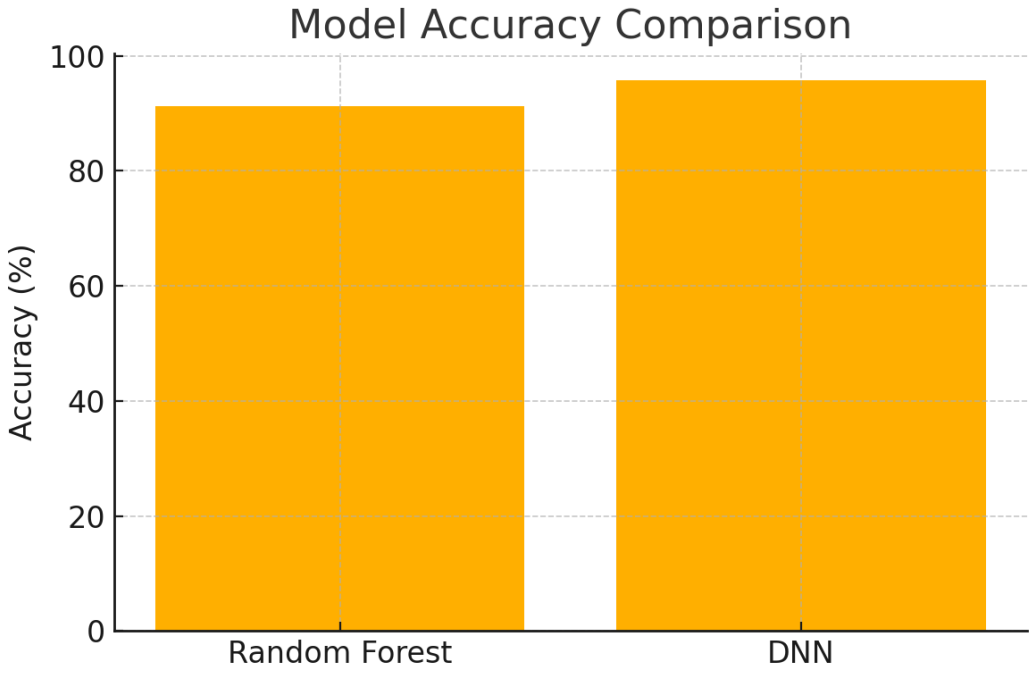

Figure 1: Model Accuracy Comparison

5. Conclusion

This study highlights the effectiveness of integrating AI-powered binary classification with automated reverse engineering for dynamic malware analysis. The proposed hybrid approach significantly reduces false positives while enhancing reverse engineering efficiency. Future work should include multi-class classification for better granularity and cross-platform analysis.

References

[1] Gaber, M. G., Ahmed, M., and Janicke, H. "Malware Detection with Artificial Intelligence: A Systematic Review." *ACM Computing Surveys*, vol. 56, no. 1, 2023.

[2] Poudyal, S., and Dasgupta, D. "Analysis of Crypto-Ransomware Using ML-Based Profiling." *IEEE Access*, vol. 9, 2021, pp. 130769–130781.

[3] Al Balawi, M., and Alnabhan, M. "Generative AI for Advanced Malware Detection." *2024 4th Intelligent Computing and Information Systems Conference (ICICIS)*, IEEE, 2024.

[4] Farzaan, M. A. M., Ghanem, M. C., and El-Hajjar, A. "AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments." *arXiv preprint arXiv:2404.05602*, 2024.

[5] Lumpatki, S. S., and Patwardhan, S. "An Overview of Artificial Intelligence Applications in Cybersecurity Domains." *International Conference on Smart Technologies and Systems for Next Generation Computing*, Springer, 2024.

[6] Jasim, S. S. "Mobile Based Malware Detection Using Artificial Intelligence Techniques: A Review." *Journal of Al-Qadisiyah for Computer Science and Mathematics*, vol. 16, no. 1, 2024, pp. 44–58.

[7] Gebrehans, G., Ilyas, N., and Eledlebi, K. "Generative Adversarial Networks for Dynamic Malware Behavior: A Comprehensive Review, Categorization, and Analysis." *IEEE Transactions on Artificial Intelligence*, 2025.

[8] Tyagi, A. K., and Addula, S. R. "Artificial Intelligence for Malware Analysis: A Systematic Study." *Artificial Intelligence–Enabled Digital Security*, Wiley, 2024.

[9] Poudyal, S., and Dasgupta, D. "AI-Powered Ransomware Detection Framework Using Reverse Engineering." *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, IEEE, 2020.

[10] Wolsey, A. "The State-of-the-Art in AI-Based Malware Detection Techniques: A Review." *arXiv preprint arXiv:2210.11239*, 2022.

[11] Lüchinger, J. "AI-Powered Ransomware to Optimize Its Impact on IoT Spectrum Sensors." Master's thesis, University of Zurich, 2023.

[12] Rohatgi, S., and Mazhar, L. "Malware Analysis and Detection: New Approaches and Techniques." *Emerging Threats and Countermeasures in Cybersecurity*, Wiley, 2025.

[13] Almomani, I., and Maglaras, L. A. "Cyber Malware: Insights into Reverse Engineering and AI-Powered Attacks." Springer, 2023.

[14] Jalaluddin, A. Z. "An Exploration of Countermeasures to Defend Against Weaponized AI Malware Exploiting Facial Recognition." PhD Dissertation, ProQuest Dissertations Publishing, 2020.