International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Malware Detection Using Artificial Intelligence

Anushka Patil
Diploma
Dept.of Computer Engineering,
PDGP, Amravati

Shreshtha Ninghot
Diploma
Dept.of Computer Engineering,
PDGP,Amravati

Astha Kuyate
Diploma
Dept.of Computer Engineering,
PDGP,Amravati

Saket Bobde
Asst.Professor
Dept.of Computer Engineering,
PDGP,Amravati

Sumit Dhopte
HOD
Dept.of Computer Engineering,
PDGP,Amravati

ABSTRACT

Malware detection is a critical issue in modern cybersecurity due to the rapid increase in sophisticated cyberattacks. Traditional detection techniques, such as signature-based methods, are often ineffective against new and evolving malware threats. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), offers advanced solutions for detecting both known and unknown malware. AI-based systems analyze large datasets, recognize hidden patterns, and identify suspicious behaviors in real time.

This paper presents a brief overview of how AI improves malware detection accuracy, reduces response time, and enhances overall cybersecurity protection.

Keywords: Artificial Intelligence, Malware Detection, Deep Learning, CNN-LSTM, Explainable AI (XAI), Adversarial Machine Learning, Zero-day Attacks, Behavioral Analysis, CIC-DGG-2025.

1. INTRODUCTION

The rapid escalation of cyber threats has rendered traditional signature-based detection systems—which rely on a static database of known file "fingerprints"—increasingly obsolete in the modern security landscape. As of 2026, the proliferation of AI-generated polymorphic malware and "living-off-the-land" attacks allows malicious code.

The integration of Machine Learning (ML) and Deep Learning (DL) enables a proactive defense posture by analyzing high-dimensional data across both static and dynamic environments.

While static analysis uses Convolutional Neural Networks (CNNs) to identify malicious textures in binary files, dynamic analysis monitors real-time system behaviors, such as unauthorized API calls or memory injections. This transition toward AI-driven security not only increases detection accuracy but also reduces the window of exposure between the release of a new threat and its neutralization.

However, the shift toward AI-centric defense has triggered an "arms race" between security researchers and cyber-adversaries. Attackers are now utilizing Generative Adversarial Networks (GANs) to craft "adversarial perturbations"—minor, non-functional code changes specifically designed to trick AI models into classifying malware as benign. This evolution necessitates the development of more robust, resilient neural architectures that can withstand data poisoning and evasion tactics.

Ultimately, the goal of modern research in malware detection is to create an autonomous, self-healing ecosystem that balances high-speed processing with interpretability. By incorporating Explainable AI (XAI) and Federated Learning, organizations can now collaborate on global threat intelligence without compromising data privacy.

Fig: Malware detection using ai

2. ARTIFICIAL INTELLIGENCE AND MALWARE

A. Artificial Intelligence:

In this section, we define Artificial Intelligence and Mal-ware. In order to give a proper scenario, we provide the classification of both AI and Malware introduced by different researchers.

The integration of Artificial Intelligence (AI) into cybersecurity marks a foundational shift from reactive, signature-based defense to proactive, predictive intelligence. Historically, malware detection relied on "digital fingerprints" or static hashes to identify threats; however, as we navigate 2026, the industrialization of polymorphic and AI-generated malware has rendered these manual databases obsolete.

AI addresses this by moving beyond simple memory toward generalized reasoning, allowing security systems to identify malicious intent through complex pattern recognition rather than exact code matches.

Within this framework, the transition from classical Machine Learning (ML) to Deep Learning (DL) has redefined the detection of "zero-day" threats. While traditional ML models require human experts to manually define malicious features (like file size or specific API calls), Deep Learning employs multi-layered Neural Networks that automatically extract and weight indicators of infection from raw data. This "feature-agnostic" approach is particularly

B. Malware:

Malicious software refers to any program or file intentionally designed to harm a computer system, network, or user. It can disrupt normal operations, steal sensitive information, gain unauthorized access, or damage data and devices.

Artificial intelligence brings significant advantages to malware detection by learning patterns directly from data rather than relying on manually crafted signatures. Machine learning models can analyze file characteristics, API call sequences, network traffic patterns, and behavioral signals to identify malicious intent even when the specific malware strain has never been seen before. This learning-based approach handles polymorphism and metamorphism better than signature databases because statistical patterns often survive code obfuscation.

AI systems can also integrate both static analysis features extracted from files without execution and dynamic features collected during sandbox execution, providing a more comprehensive detection capability than either approach alone.

3. IMPACT ON MALWARE DETECTION USING AI

Artificial Intelligence (AI) has significantly transformed malware detection by improving accuracy, speed, and efficiency in identifying cyber threats.

Unlike traditional signature-based methods, AI uses machine learning algorithms to analyze patterns and system behavior, enabling the detection of new and unknown (zero-day) malware.

It provides real-time monitoring and automatic threat response, reducing the time between detection and action. AI systems continuously learn from new data, which helps minimize false positives and improve overall reliability. As a result, organizations benefit from stronger cybersecurity protection and faster incident response.

4. ENHANCING MALWARE DETECTION

-Behavioral Fingerprinting: Instead of looking at what a file *is*, systems analyze what it *does*. For example, a PowerShell script might be legitimate, but if it starts dumping credentials, behavioral engines flag the intent as malicious.
-Living off the Land" (LotL): Attackers stopped bringing their own tools; they now use your tools (like PowerShell or Terminal) against you.
-The Fix: Behavioral Fingerprinting. We don't care what the file looks like; we care what it does. If a Calculator app starts encrypted files, it's malware, period.
-Contextual Awareness: Systems now track "chains of events." A single command might look safe, but if it follows a suspicious download and leads to a password change, the AI connects the dot

5. CHALLENGES AND ETHICAL CONSIDERATION

Following that same structure, here are the Challenges and Ethical Considerations for enhancing malware detection :

-Privacy vs. Visibility: To catch "fileless" or behavioral threats, AI systems require deep access to user activity, keystrokes, and encrypted traffic. This constant monitoring creates a thin line between enterprise security and invasive workplace surveillance.
-Algorithmic Bias and False Positives: AI models trained on narrow datasets may flag legitimate, non-standard coding styles or remote-work patterns as "malicious." This can lead to unfair lockouts or disciplinary actions against specific demographic groups or specialized roles.
- The "Black Box" Accountability Gap: Deep learning models often lack transparency. When an autonomous system shuts down a critical server or denies a user access, it can be difficult for human analysts to explain the "why" to stakeholders or regulators.
-Adversarial AI (Dual-Use): The same breakthroughs used to detect malware are being used by attackers to "train" their code to bypass those very defenses. This creates an endless arms race where a single leaked detection model can be used to engineer invisible malware.

6. FUTURE PROSPECTS

The future of malware detection and cybersecurity is characterized by continuous innovation and the adoption of intelligent defense mechanisms:

- Predictive Threat Hunting: Instead of waiting for an alert, AI models now perform "Continuous Exposure Management." They proactively simulate 10,000 attack paths per second to find and patch "logic flaws" before a hacker can exploit them.
- The "Post-Malware" Truth Layer: As malware becomes invisible by using legitimate tools (Living-off-the-Land), detection focuses on a Truth Layer. This correlates network movement, identity signals, and hardware metadata to spot "malicious intent" even when the code itself looks clean.
- Quantum-Resistant Detection: With cryptographic deadlines approaching (2030), forward-leaning systems are already piloting Post-Quantum Authentication. This ensures that "Harvest Now, Decrypt Later" attacks don't render today's encrypted malware samples readable in the future.

7. CONCLUSIONS

That traditional signature-based methods might miss, while also excelling at analyzing patterns and behaviors to detect malicious activity in obfuscated or polymorphic malware. Additionally, automation helps security teams handle the vast volume of threats more efficiently, reducing manual effort. However, challenges remain, including false positives where AI systems may flag legitimate software as malicious, the risk of adversarial attacks where cybercriminals use AI to create malware that evades detection, and the data dependency of models that require large, diverse datasets for training. In conclusion, AI is a powerful tool in the ongoing battle against malware, offering proactive and dynamic detection capabilities. However, it should be integrated with traditional security methods and human expertise for the most robust defense, and ongoing research and adaptation are essential to stay ahead of evolving threats.

ACKNOWLEDGEMENT

The authors would like to thank their mentors and institutions for guidance and support in preparing this manuscript.

REFERENCES

[1] O. Asaolu, "On the emergence of new computer technologies," Educational Technology Society, vol. 9, pp. 335–343, 2006.

[2] Z. Arsic and B. Milovanovic, "Importance of computer technology in realization of cultural and educational tasks of preschool institutions," International Journal of Cognitive Research in Science, Engineering and Education, vol. 4, pp. 9–15, 2016.

[3] A. P. Gilakjani, "A detailed analysis over some important issues towards using computer technology into the EFL classrooms," Universal Journal of Educational Research, vol. 2, pp. 146–153, 2014.

[4] H. F. Md Jobair et al., "Smart connected aircraft: Towards security, privacy, and ethical hacking," International Conference on Security of Information and Networks, 2022.

[5] S. Subramanya and N. Lakshminarasimhan, "Computer viruses," IEEE Potentials, vol. 20, pp. 16–19, 2001.

[6] S. Levy and J. Crandall, "The program with a personality: Analysis of Elk Cloner, the first personal computer virus," 2020.

[7] N. Milosevic, "History of malware," 2013.

[8] A. P. Namanya et al., "The world of malware: An overview," 2018.

[9] I. Khan, "An introduction to computer viruses: Problems and solutions," Library Hi Tech News, vol. 29, pp. 8–12, 2012.

[10] M. Bishop, "An overview of computer viruses in a research environment," Tech. Rep., USA, 1991.