International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 6, Nov-Dec-2026, ISSN (Online): 2395-566X

A Study on Malware Detection Techniques and Their Effectiveness

Mahak S. Patel
Department Of Artificial Intelligence And Data Science
Sahyadri Valley College Of Engineering & Technology,Rajuri Pune, India
Email: Mahif021218@Gmail.Com

Abstract – Malware, also known as malicious software, is one of the major threats to computer systems and networks. It includes viruses, worms, trojans, ransomware, and spyware. Malware can damage computer systems, steal sensitive information, and affect data security. Therefore, malware detection plays an important role in cybersecurity. This paper presents a study of different malware detection techniques, including signature-based detection, static analysis, dynamic analysis, and machine learning-based detection. It discusses their working principles, advantages, and limitations. The study also examines how machine learning techniques can help identify suspicious and previously unseen malware. The objective is to understand existing malware detection approaches and their effectiveness in improving computer system security.

Keywords — Malware Detection, Cybersecurity, Machine Learning, Static Analysis, Dynamic Analysis.

I. INTRODUCTION

Malware, also known as malicious software, is one of the major security threats in modern computer systems. It is designed to damage computer systems, steal sensitive information, disrupt network operations, and gain unauthorized access to devices. Common types of malware include viruses, worms, Trojan horses, ransomware, spyware, and rootkits.

With the rapid growth of internet usage and digital technologies, malware attacks have become a serious concern for individuals and organizations. These attacks can cause data loss, financial damage, privacy violations, and system failures. Therefore, malware detection plays an important role in maintaining computer security.

Malware detection is the process of identifying malicious programs and suspicious activities in a computer system. Traditional antivirus software mainly uses signature-based detection to identify previously known malware. However, this technique may not effectively detect new or modified malware.

To overcome these limitations, different techniques such as static analysis, dynamic analysis, behavior-based detection, and machine learning-based detection are used. These techniques help identify suspicious files and activities.

The main objective of this paper is to study different malware detection techniques, understand their working principles, compare their advantages and limitations, and examine the role of machine learning in improving malware detection.

II. LITERATURE REVIEW

Several researchers have conducted studies on malware detection to improve computer system security.

Souri and Hosseini (2018) presented a survey of malware detection approaches using data mining techniques. Their research discussed different detection methods and the application of machine learning techniques for identifying malicious software.

Ucci, Aniello, and Baldoni (2019) presented a survey of machine learning techniques for malware analysis. Their study discussed machine learning algorithms, malware features, datasets, and challenges associated with malware detection.

Traditional signature-based detection techniques are commonly used to identify known malware. However, these techniques have limitations when dealing with new and modified malware.

Recent research has also focused on static analysis and dynamic analysis techniques. Static analysis examines files without executing them, whereas dynamic analysis observes program behavior during execution.

Machine learning-based approaches have gained attention because they can identify patterns from malware datasets and help classify suspicious files.

© 2026 IJSRET

The literature indicates that combining different malware detection techniques can provide a more comprehensive approach to identifying malicious software.

III. PROPOSED METHODOLOGY

The proposed methodology focuses on studying and understanding different techniques used for malware detection. It includes the following stages:

- **Data Collection:** Malware and benign file information can be collected from publicly available datasets for research and analysis.
- **Data Preprocessing**: The collected data is cleaned and prepared for analysis. Irrelevant information and duplicate records can be removed.
- **Feature Extraction**: Important features such as file size, file type, file characteristics, and behavioral information are identified for malware analysis.
- **Malware Detection:** Detection techniques such as signature-based analysis, static analysis, dynamic analysis, and machine learning can be applied to identify suspicious files.
- **Classification:** Machine learning algorithms such as Decision Tree, Random Forest, and Support Vector Machine can be studied to classify files into malware and benign categories.
- **Evaluation**: The performance of a detection model can be evaluated using measures such as accuracy, precision, recall, and F1-score. Actual evaluation results should be included only after conducting experiments.

The overall methodology provides a structured approach to understanding malware detection and the application of machine learning techniques in cybersecurity.

Figures and tables are important components of the malware detection system as they help explain the working process and comparison of different detection techniques. Figures provide a visual representation of the system workflow, while tables present information in a structured and understandable format.

The malware detection process consists of several stages, including input file collection, data preprocessing, feature extraction, detection, classification, and generation of the final report.

2. **Workflow of Malware Detection System**

The workflow illustrates the different stages involved in identifying malicious files. The input files are collected and processed to extract relevant features. The detection engine analyzes the extracted information and classifies files into benign or malware categories. Finally, the system generates an alert or report based on the detection result.

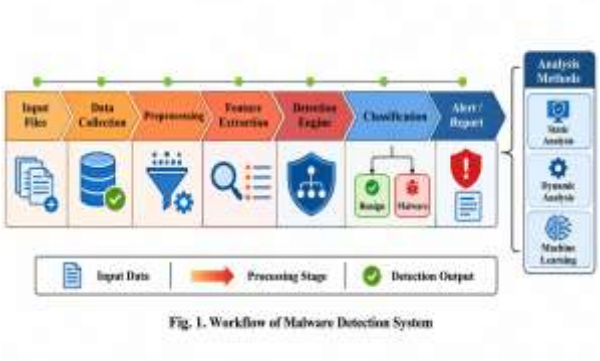

Fig. 1. Workflow of Malware Detection System

3. **Table Captions**

Tables are numbered consecutively and their captions are placed above the corresponding tables. Tables are used to compare different malware detection techniques based on their working principles, advantages, and limitations.

1. Figures And Tables

Table I: Comparison of Malware Detection Techniques

Sr. No.	Malware Detection Techniques		
	Detection Technique	Worki ng Princi ple	Limitations
I.	Signature-Based Detection	Matche s known malwar e signatu res	Cannot easily detect new malware
II.	Static Analysis	Exami nes files withou t executi on	Affected by code obfuscation
III.	Dynamic Analysis	Observes progrm behavior during execution	Requires more resources
IV.	Machine Learning	Learns pattern s from dataset s	Depends on training data
V.	Hybrid Detection	Combines multiple **techniques**	Complex implementation

© 2026 IJSRET

4. Some Helpful Hints

1. Malware Detection Evaluation
Malware detection systems are evaluated using different performance metrics to understand their effectiveness. Common evaluation metrics include Accuracy, Precision, Recall, and F1-Score. These metrics help measure how effectively a detection model identifies malicious and benign files.

The following equations are commonly used for evaluating malware detection models:

Accuracy:
Accuracy = (TP + TN) / (TP + TN + FP + FN) … (1)
Precision:
Precision = TP / (TP + FP) … (2)
Recall:
Recall = TP / (TP + FN) … (3)
F1-Score:
F1-Score = 2 × (Precision × Recall) / (Precision + Recall) …(4)
Where:
TP = True Positive
TN = True Negative
FP = False Positive
FN=False Negative

2. Abbreviations and Acronyms
The following abbreviations are commonly used in malware detection and cybersecurity research. Their full forms are provided for better understanding.

- **ML:** Machine Learning
- **AI:** Artificial Intelligence
- **AV**: Antivirus
- **API:** Application Programming Interface
- **IDS:** Intrusion Detection System
- **TP:** True Positive
- **TN:** True Negative
- **FP:** False Positive
- **FN:** False Negative
- **FPR**: False Positive Rate

All abbreviations should be defined when they first appear in the main text of the research paper.

IV. CONCLUSION

Malware detection is an important part of modern cybersecurity. This paper studied different malware detection techniques, including signature-based detection, static analysis, dynamic analysis, machine learning-based detection, and hybrid analysis.

Each technique has its own advantages and limitations. Traditional methods are useful for identifying known threats, whereas machine learning and behavior-based approaches provide additional possibilities for detecting suspicious activities.

The study concludes that combining different malware detection approaches can support more comprehensive and reliable security systems. Future research can focus on improving detection of unknown malware, real-time monitoring, and efficient machine learning models.

1. Appendix

The appendix provides additional information related to the malware detection techniques discussed in this research paper.

1.Common Malware Categories

The following are some common categories of malware:

- **Virus:** Malicious software that attaches itself to other files or programs.
- **Worm:** Malware that can spread between computer systems.
- **Trojan Horse:** Malicious software that disguises itself as legitimate software.
- **Ransomware:** Malware that restricts access to data and demands payment.
- **Spyware:** Software designed to collect information without proper authorization.

2. Malware Detection Evaluation Terms

- **TP (True Positive):** Malware correctly identified as malicious.
- **TN (True Negative):** Benign files correctly identified as safe.
- **FP (False Positive):** Benign files incorrectly identified as malicious.
- **FN (False Negative):** Malware incorrectly identified as benign.

3. Detection Techniques
The major techniques discussed in this paper include signature-based detection, static analysis, dynamic analysis, and machine learning-based detection. These techniques

© 2026 IJSRET

help identify suspicious files and improve computer system security.

4. Acknowledgment

I would like to express my sincere gratitude to my project guide for providing valuable guidance, continuous support, and encouragement throughout the preparation of this research paper on “Malware Detection”.

I am thankful to the Head of the Department of Artificial Intelligence and Data Science and all faculty members of Sahyadri Valley College of Engineering & Technology, Rajuri, for their valuable suggestions and support.

I would also like to thank my college for providing the necessary resources and academic environment to

complete this research paper.Finally, I would like to express my gratitude to my parents, friends, and everyone who directly or indirectly supported me in completing this research work.

REFERENCES

1. A. Souri and R. Hosseini, "A State-of-the-Art Survey of Malware Detection Approaches Using Data Mining Techniques," Human-centric Computing and Information Sciences, vol. 8, article 3, 2018. DOI: 10.1186/s13673-018-0125-x.
2. D. Ucci, L. Aniello, and R. Baldoni, "Survey of Machine Learning Techniques for Malware Analysis," Computers & Security, vol. 81, pp. 123–147, 2019. DOI: 10.1016/j.cose.2018.11.001.
3. "Bridging Static and Dynamic Frontiers: A Systematic Review of Malware Detection Techniques," IEEE, 2025. DOI: 10.1109/IETC64455.2025.11039456.

© 2026 IJSRET