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 6, Issue 10, March 2026
Impact Factor: 8.2

An Intelligent Approach for Classifying and Eliminating Malware in Modern Computing Environments

Kajal Jaisinghani and Dr. Santosh Singh
Research Scholar, UDIT, University of Mumbai, Mumbai
PhD Guide, University of Mumbai, Mumbai

Abstract: *Malware has become one of the most serious threats to modern computing systems, affecting individuals, organizations, and governments. Traditional signature-based security mechanisms are no longer sufficient to detect advanced and evolving malware attacks. This research paper presents an intelligent approach for the classification and elimination of malware using machine learning techniques. The proposed approach focuses on analyzing malware behavior and features to accurately classify malicious software and eliminate it effectively. Experimental analysis shows that intelligent malware detection techniques provide better accuracy, adaptability, and real-time protection compared to conventional methods.*

Keywords:*Malware Detection, Machine Learning, Cyber Security, Malware Classification, Intelligent Systems.*

I. INTRODUCTION

With the rapid growth of the internet and digital technologies, cyber threats have increased significantly. Malware, short for malicious software, is designed to disrupt systems, steal sensitive data, or gain unauthorized access. Common types of malware include viruses, worms, trojans, ransomware, spyware, and adware.

Traditional antivirus systems rely heavily on signature-based detection, which fails against new or unknown malware variants. As cyber attackers continuously modify malware to evade detection, there is a growing need for intelligent and adaptive security solutions. This paper explores an intelligent approach using machine learning techniques for malware classification and elimination.

II. TYPES OF MALWARE

Malware can be broadly classified into the following categories:

- **Virus:** Attaches itself to legitimate files and spreads when executed.
- **Worm:** Self-replicates and spreads across networks without user interaction.
- **Trojan Horse:** Disguises itself as legitimate software.
- **Ransomware:** Encrypts user data and demands payment for recovery.
- **Spyware:** Secretly monitors user activities.
- **Adware:** Displays unwanted advertisements and collects user data.

Understanding these categories helps in designing effective classification models.

III. CHALLENGES IN MALWARE DETECTION

Malware detection faces several challenges:

- Rapid evolution of malware variants
- Use of obfuscation and encryption techniques

DOI: 10.48175/IJARSCT-35003

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 6, Issue 10, March 2026
Impact Factor: 8.2

- Zero-day attacks
- High false positive rates
- Resource constraints in real-time systems

These challenges necessitate the use of intelligent techniques that can learn and adapt dynamically.

IV. INTELLIGENT MALWARE CLASSIFICATION APPROACH

4.1 Feature Extraction

The first step involves extracting relevant features from executable files. These include:

- File size and structure
- Opcode sequences
- API call patterns
- Network behavior
- System resource usage

4.2 Machine Learning Models

The extracted features are fed into machine learning classifiers such as:

- Decision Trees
- Random Forest
- Support Vector Machine (SVM)
- Naïve Bayes
- Neural Networks

These models learn patterns that distinguish malicious files from benign ones.

4.3 Classification Process

The trained model classifies input files into malware categories or as benign software. Machine learning enables detection of previously unseen malware based on behavior rather than known signatures.

V. MALWARE ELIMINATION TECHNIQUES

Once malware is detected and classified, elimination strategies are applied:

- Automatic quarantine of infected files
- Removal or repair of malicious code
- Blocking malicious processes and network connections
- Restoring system settings to a secure state
- Integration of detection and elimination ensures complete system protection.

VI. EXPERIMENTAL ANALYSIS

The intelligent approach was tested using a dataset containing both benign and malicious samples. The results showed:

- Higher detection accuracy compared to traditional antivirus systems
- Reduced false positive rates
- Improved detection of zero-day malware
- Faster response time
- Machine learning-based systems demonstrated strong adaptability and robustness

VII. ADVANTAGES OF THE PROPOSED APPROACH

- Detects unknown and evolving malware

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 6, Issue 10, March 2026
Impact Factor: 8.2

- Reduces dependency on signature updates
- Provides real-time protection
- Scalable for large networks
- Improves overall system security

VIII. LIMITATIONS

- Despite its advantages, the approach has some limitations:
- Requires large and high-quality datasets
- Computational overhead during training
- Model performance depends on feature selection

These limitations can be addressed with optimized models and hardware support.

XI. FUTURE SCOPE

- Future research can focus on:
- Deep learning-based malware detection
- Cloud-based malware analysis
- AI-driven autonomous security systems
- Integration with Internet of Things (IoT) security
- Real-time adaptive defense mechanisms

X. CONCLUSION

This research paper presented an intelligent approach for classifying and eliminating malware using machine learning techniques. The study highlights that intelligent systems outperform traditional signature-based methods in terms of accuracy, adaptability, and efficiency. With the increasing complexity of cyber threats, intelligent malware detection and elimination techniques are essential for ensuring secure computing environments.

REFERENCES

1. Anderson, B., & Roth, P. (2018). EMBER: An open dataset for training static PE malware machine learning models.
2. Kumar, S., & Singh, A. (2020). Machine learning approaches for malware classification.
3. Shabtai, A., Elovici, Y., & Rokach, L. (2012). A survey of data-driven methods for malware detection.
4. Ye, Y., Li, T., Jiang, Q., & Wang, Y. (2017). Intelligent malware detection using machine learning.