9IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 13, Issue 2, April-May 2025
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Intelligent Anti-Malware System Using Deep Learning

Subanu M[1], Swathi S[2], Siva Harini E[3], Udhayanithi N[4] and Asst.Prof Ramya C[5]

[1]Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613 006, India
msubanusuba@gmail.com

[2]Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613 006, India
Swathi562003@gmail.com

[3]Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613 006, India
sivaharinielangovan@gmail.com

[4] Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613 006, India
udhayanithiseliyan@gmail.com@gmail.com

[5]Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu 613 006, India
V.ramya81@gmail.com

Abstract

The exponential rise of sophisticated cyber threats, particularly malware, necessitates the development of intelligent, adaptive, and proactive detection mechanisms. Traditional signature-based antivirus solutions are becoming ineffective as they fail to dynamically adapt to newly emerging malware variants and lack real-time mitigation capabilities. Existing detection methodologies, including Generative Adversarial Networks (GAN) and Support Vector Machines (SVM), struggle with accurately classifying novel cyber threats due to their limited generalization ability. To address these challenges, our proposed system leverages Deep Learning (DL)models, integrating Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Random Forest classifiers. This system not only detects and mitigates malware based on behavioral and structural analysis but also continuously learns from newly identified threats, autonomously retraining DL models for enhanced future detection. Additionally, our approach incorporates automated threat removal, ensuring real-time system protection

Keywords: Malware Detection, Deep Learning, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Random Forest, Threat Mit

1. INTRODUCTION

The increasing complexity of cyber threats necessitates advanced malware detection systems beyond traditional signature-based antivirus solutions. With the rise of

ransomware zero-day attacks, and polymorphic malware, static detection techniques have proven insufficient in mitigating evolving threats.based and heuristic approaches, often fail to detect malware variants that modify their structure to evade Additionally, traditional password-based security mechanisms are vulnerable to brute-force attacks and credential theft, making endpoints and enterprise systems susceptible to exploitation.

To combat these security challenges, this research introduces an intelligent anti-malware system that leverages

deep learning to dynamically identify and mitigate threats. Our system integrates behavioral analysis, deep learning-based threat detection, and automated malware neutralization to enhance system security. The proposed approach effectively detects emerging malware by utilizing CNN, LSTM, and Random Forest classifiers to identify malicious patterns in files, system processes, and network activity. Furthermore, our self-learning mechanism continuously updates the system by training deep learning models with new threat patterns, ensuring future malware variants can be identified proactively.

This research aims to develop a proactive, self-learning, and intelligent anti-malware solution that significantly improves detection accuracy and response time, ultimately strengthening cybersecurity This make our system more efficient and accurate in detection and restriction of malwares.

2. LITERATURE SURVEY

Mohamed Belaoued, Abdelouahid Derhab,[1] Macomal: Multi-agent Anti-malware Assistance In this paper, we propose MACoMal, a multi-agent-based decision mechanism, which assists heterogeneous anti-malware tools to collaborate with each other in order to reach a consensual decision about the maliciousness of a suspicious file. MACoMal consists of two main elements: (1) an executable file identification model, and (2) a collaborative decision-making scheme. MACoMal is analyzed with respect to network connectivity and global decision correctness.

Minho Kim [2]Ev detector: Anti-analysis In Malware. These detectors are designed to help malware identify when it is running in a controlled environment, such as a sandbox or virtual machine, commonly used for malware analysis. To evade detection, malware employs sophisticated methods like system fingerprinting, where it checks for unique identifiers associated with virtual environments, and timing attacks, which alter the behaviour of the malware based on the speed or performance of the system it is running on. Additionally, resource checks are often used to detect discrepancies in CPU, memory, and other system resources that differ from those of typical user machines.

Faiza Babar Khan[3], we have developed an integrated Anti-Malware System (AMS) architecture that incorporates both conventional signature-based detection and AI-based detection modules. Our approach employs a Generative Adversarial Network (GAN) based Malware Classifier Optimizer (MCOGAN) framework, which can optimize a malware classifier. This framework utilizes GANs to generate fabricated benign files that can be used to train external discriminators for optimization purposes. We describe our proposed framework and anti-malware system in detail to provide a better understanding of how a malware detection system works

3. PROPOSED MODEL

In the modern digital era, cybersecurity threats have become more sophisticated, posing significant risks to personal and enterprise systems. Traditional malware detection mechanisms struggle to counter rapidly evolving cyber threats, including zero-day exploits, polymorphic malware, and ransomware. Conventional antivirus solutions rely on static detection techniques, which are ineffective in identifying novel and obfuscated threats.

To address these challenges, we propose an Intelligent Anti-Malware System that enhances security through advanced Deep Learning (DL) and Machine Learning (ML) models. Our model integrates:

1.Behavior-Based Threat Detection – Identifies malware based on execution patterns and anomalies.
2.Automated Deep Learning Training – Continuously learns from new threats and retrains models for improved future identification.
3.Real-Time Threat Mitigation – Actively removes detected malware and prevents further system compromise

By leveraging CNN, LSTM, and Random Forest classifiers, our system moves beyond static detection, ensuring adaptive, intelligent, and proactive malware defense

A. THREAT IDENTIFICATION AND ANALYSIS

The Threat Identification Module is the first step in detecting malicious activities within a system. When a file or application is accessed, the system extracts its features, including:

1.Code Analysis – Evaluates the structure and patterns of the executable.
2.Behavioral Monitoring – Tracks file execution, API calls, and resource utilization.
3.Anomaly Detection – Identifies deviations from normal system behavior.

Using deep learning models, the system continuously refines its threat detection process, allowing it to classify both known and unknown malware variants effectively.

B. SYSTEM PROTECTION AND RESPONSE

The System Protection Module ensures real-time security by taking immediate actions upon detecting a threat. If malware is identified, the system:

1.Blocks malicious execution to prevent system infection.
2.Isolates the infected file in a secure environment for further analysis.
3.Automatically removes threats and mitigates potential damage.

Our system addresses this by:
1.Deobfuscating code structures using deep learning-based reverse engineering techniques.
2.Identifying hidden malware behaviors by monitoring execution in a controlled environment.
3.Detecting polymorphic malware by recognizing behavioral similarities rather than relying on static signatures.
By incorporating advanced AI-driven techniques, our system enhances its ability to detect and neutralize even the most sophisticated malware variants.

4. CONCLUSION

The Intelligent Anti-Malware System Using Deep Learning provides a self-learning, adaptive, and real-time malware detection framework. By integrating CNN, LSTM, and Random Forest classifiers, the system offers superior threat detection, dynamic learning, and proactive security measures This ensures enhanced cybersecurity protection, minimizing the risks posed by evolving malware threat.

REFERENCES

1.Mohamed Belaoued, Abdelouahid Derhab, Smaine Mazouzi (2020). Macomal: Multi-agent Anti-malware Assistance. Utilizes Multi-agent Systems (MAS) and Reinforcement Learning to improve malware detection accuracy through collaboration. However, it faces scalability issues and potential overhead in coordination.

2. EV Detector: Anti-analysis in Malware" by Minho Kim, Haehyun Cho, and Jeong Hyun Yi (2022) explores API-based tracing buffer analysis to detect anti-analysis techniques used in modern malware. The study highlights the effectiveness of API monitoring for malware detection but notes limitations handling sophisticated obfuscation methods.

3. Survey on Adversarial Attacks for Malware Analysis" by Kshitiz Aryal, Maanak Gupta, Mahmoud Abd Elsala, and Pradip Kunwar (2024) explores adversarial evasion techniques in malware using machine learning models. The study provides a comprehensive review of adversarial machine learning frameworks such as CleverHans and Foolbox. The research highlights the impact of adversarial perturbations on malware detection systems but lacks focus on countermeasure strategies.

4.Generates alerts and reports for user awareness and forensic analysis.
4.Generative Adversarial Network-Based Malware Classifier" by Faiza Babar Khan, Muhammad Hanif Durad, and Asifullah Khan (2024) presents a malware classification model leveraging Generative Adversarial Networks (GANs). The study employs TensorFlow and PyTorch for training GAN-based classifiers, demonstrating improved adaptability to emerging malware variants. However, the model's susceptibility to false positives and high computational overhead remains a challenge.

By incorporating real-time deep learning-based threat detection, our system ensures that even previously unseen malware variants can be detected and neutralized before they cause harm

C. DYNAMIC THREAT LEARNING AND MODEL TRAINING

To further enhance malware detection capabilities, the system includes an automated training module that continuously improves its deep learning models. When new malware is detected:

1.The extracted features and behavioral data are analyzed and stored in a secure database.

2.The deep learning models (CNN, LSTM) are updated with the new data to improve detection accuracy.

3.Threat intelligence reports are generated, providing insights into emerging attack patterns.