AI BASED THREAT DETECTION AND THREAT ELIMINATION TO BLOCK CRYPTO RANSOMWARE

Project Reference No.: *49S_BE_6031*

College : REVA University, Bengaluru
Branch : Department of Electronics and Communication Engineering
Guide : Prof. Dilip Chandra E
Students(s) : Ms. Aditi Rao E A
Ms. Bindhu Shree S
Ms. Harshitha C V
Ms. Kavya N

Keywords:
Artificial Intelligence, Malware Detection, Cybersecurity, Machine Learning, Threat Prevention, Random Forest, Real-Time Monitoring.

Introduction:

The AI-driven malware threat detection and prevention system offers a smart and dynamic security landscape that safeguards the current computing and network systems. By simulating and learning the variety of different attack patterns and system behaviours, it allows organizations and users to monitor, analyse and respond to cyber threats in real time. Through assistance of AI threat detection feature, security administrators can formulate policies and deploy models that would continuously monitor system activities asper the needs of the operations and risk approach. Security mechanisms powered by AI improve automated decision making and improve incident response. It enhances the communication between mitigation and detection aspects. Individual detection models are trained with distinct goals i.e., detecting ransomware, trojans, spyware or zero-day malware which the system tries to detect and halt at the initial stages of execution. The role of AI-based threat detection in system assessment during cybersecurity platforms in which various data sources (host logs, network traffic, and application activities)are included is quite vital in evaluating the effectiveness and strength of security components. Given systems to simulated and realistic attack scenarios, the framework allows detecting the accuracy of detection, false alarms, resource efficiency, and response efficiency. The AI-based analysis aids in enhancing defensive strategies, deployment decisions, and resilience of the current infrastructures to the emerging malware attacks.

Objectives:

1. Design and implement a machine learning framework capable of identifying malicious files and behaviours using intelligent analysis techniques.
2. Monitor file operations, process behaviour, API calls, and network traffic patterns to detect suspicious or malicious activities in real time.

3. Identify and categorize malware such as ransomware, trojans, spyware, worms, rootkits, adware, and crypto miners using AI models and rule-based analysis.
4. Enable real-time response actions including file quarantine, blocking malicious execution, and alert notifications to minimize system damage.

Methodology:

The malware detection and prevention system, which is proposed based on AI, is built with a modular architecture and consists of four modules: Feature Extraction Engine, AI Detection Model, Prevention Module, and Web Interface. A feature vector with 2381 dimensions is extracted by the system when a file is scanned using the raw file bytes and features comprising of the EMBER 2018 Dataset. A Random Forest classifier with scikit-learn is used to analyse these features to estimate the probability of malware. The malware types recognized by the system are also ransomware, trojan, spyware, worm, rootkit, adware, and crypto miner, which is determined by the rule-based analysis of the keywords. Upon the detection of malware, the prevention module will automatically quarantine the file, issue an email notification, and record the output in a web dashboard.

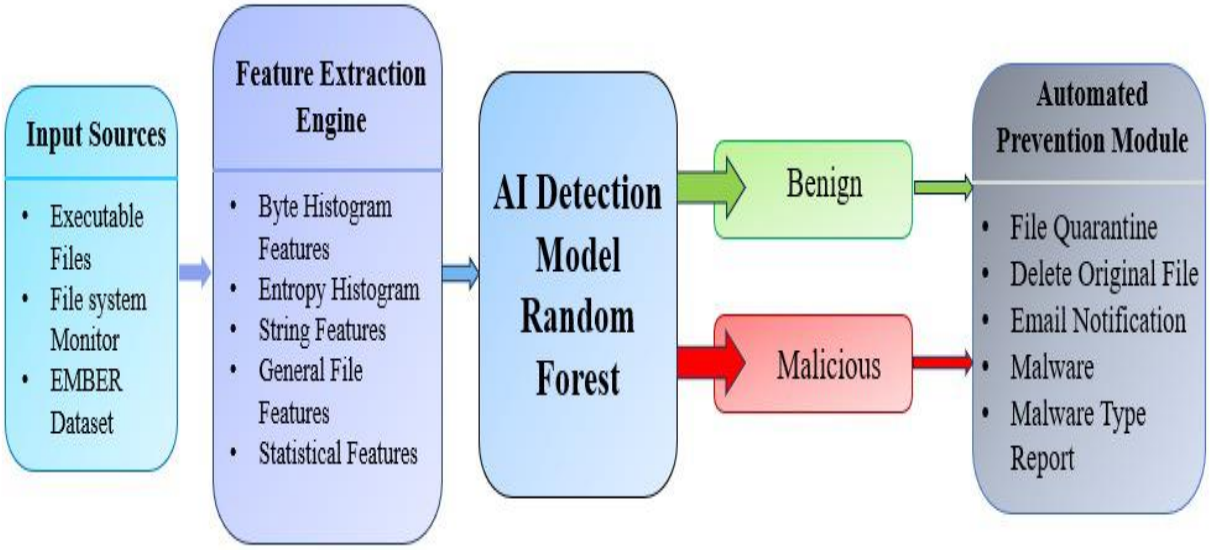

Figure 1: AI-based Malware Detection and Prevention Framework.

Result and Conclusion:

The proposed AI-based malware detection and prevention system was implemented and evaluated using the EMBER 2018 dataset. The Random Forest classifier effectively distinguished between benign and malicious files using extracted behavioural and structural features. The system achieved high detection accuracy with a low false positive rate, ensuring reliable threat identification. Real-time monitoring enabled fast file scanning, while the prevention module quarantined malicious files before execution. Automated email alerts and a web dashboard provided clear monitoring and reporting of detected threats and system activities.

References:

[1] J. Numpradit, P. Boonyopakorn, and S. Charoensawat, “Malware Detection and Analysis Using Deep Learning through Fully Connected Neural Network (FCNN),” in IEEE International Conference on Cybernetics and Innovations (ICCI), 2025.

[2] N. Parihar, A. Tyagi, P. Fernandes, M. Tiwari, S. Tyagi, and A. Y. A. B. Ahmad, “Using Machine Learning to Enhance Cybersecurity Threat Detection,” in International Conference on Pervasive Computational Technologies (ICPCT), 2025.

[3] K. Sandya, T. S. K. Sharma, G. V. Reddy, and M. H. Kumar, “Malware Detection System: Safeguarding Against Evolving Threats,” in International Conference on Expert Clouds and Applications (ICOECA), 2025.

[4] T. Desai and R. K. Pal, “Machine Learning in Cybersecurity: A Comprehensive Review of Threat Detection, Prevention, and Response Strategies,” in International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), 2025.

Future Scope:

The future scope of this project includes:

1. Integration of advanced deep learning models to improve malware detection accuracy.
2. Deployment of the system in cloud environments for centralized and scalable security monitoring.
3. Extension of malware detection support to mobile and IoT devices.
4. Implementation of adaptive self-learning mechanisms for detecting emerging and zero-day threats.