Team 2.11 13/10/2023
Team members- Hiya Sharma
Shashibhushan Das
Athibhan Pruthvi
Mohan Raj

Malware Classification and Detection

Abstract

Malware continues to be a significant cybersecurity threat, with an ever-evolving landscape of malicious software that poses risks to computer systems, networks, and personal data. To combat this threat, the project aims to develop machine learning models for the accurate classification of diverse malware types, implement real-time detection in files and network traffic, provide a user-friendly interface for security professionals, ensure robust data collection, enable continuous learning from new threats, rigorously evaluate model performance, enhance information security, and foster ongoing research and development in the field to effectively combat the evolving landscape of cybersecurity threats.

The methods employed in this project encompass data collection and preprocessing, feature engineering, training machine learning models, real-time detection integration, user interface development, continuous learning design, performance evaluation, and a focus on enhancing information security. These methods collectively form the foundation for achieving the project's objectives in malware classification and detection.

The primary objective of this project is to build a model capable of identifying and categorizing malware into various types, such as viruses, trojans, ransomware, spyware, and more. This classification will enable security professionals to better understand the nature of the malware they encounter, thereby enhancing incident response and preventive measures.

The project offers several key benefits, including enhanced information security, proactive threat mitigation, and precise malware identification. It empowers security professionals with advanced tools, streamlines decision-making through a user-friendly interface, and supports ongoing research to stay ahead of evolving cybersecurity threats, ultimately contributing to a safer and more secure digital environment. It is poised to yield significant advancements in enhancing cybersecurity practices. Through our interdisciplinary approach, we are on track to successfully design, develop, and implement a sophisticated system for identifying and classifying malware, ultimately mitigating the risks posed by these perpetually evolving digital threats.

Keywords- Malware, cybersecurity, machine learning models, classification, real-time detection, information security, threat mitigation, incident response, preventive measures