Abstract

A computer system or network can be damaged by malware, which is malicious software. It may take the shape of viruses, worms, trojan horses, malware, or ransomware, among others. Malware has the ability to destroy files, steal data, and even take over a computer system.

Many contemporary malware strains are now resistant to conventional malware detection techniques like signature-based detection. These strains are capable of avoiding identification because they frequently alter their signatures.

A promising method for classifying and detecting malware is machine learning (ML). To learn the features of malware, ML systems can be trained on a sizable collection of malicious and benign samples. This information can then be applied to identify fresh and undiscovered malware strains.

This research suggests a fresh malware detection and categorization method based on machine learning. A substantial dataset of malicious and benign samples will be used to train the system. It will then employ this information to identify and categorize fresh malware strains.

A number of criteria, including accuracy, precision, recall, and F1 score, will be used to assess the system. Additionally, it will be evaluated against current malware detection and classification systems.

A strong and efficient ML-based malware detection and categorization system is the project's anticipated output. Even if the malware strains are created to avoid conventional detection techniques, our system will be able to identify and categorize new and unidentified malware strains.

A wide range of stakeholders, including people, businesses, and governments, will profit from the system. It can be employed to defend computer systems from malware assaults as well as to look into and bring charges against malware authors.