Title: Ransomware Attack Detection using Machine Learning Approaches

Author Names: Md Shazzadur Rahman; Md Sayeed Ahmed Sabbir; Sudipto Ghosh

Abstract: Ransomware attacks have become one of the most prevalent and concerning cybersecurity threats in recent years. Traditional signature-based antivirus solutions are struggling to keep up with the evolving sophistication of ransomware, necessitating the development of more advanced detection methods. Malware has always been a menace to organizations, but timely infection detection is still difficult. By performing meaningless actions that strain the system and keep it from working effectively, malware can quickly harm it. Malware can be found using either the behavior-based technique or the conventional method, which depends on the malware's signature. When the virus is active in the computer, it performs operating system tasks and downloads infected files from the internet, among other acts that define its activity. The suggested method discovers the infection based on how it acts. In this study, a combination of support vector machines and principal component analysis is proposed as the model. Our suggested model correctly identified real malware with a decision tree accuracy of 0.995, an SVM accuracy of 0.787, and a random accuracy of 0.997. Organizations have always been at risk from malware, but early virus detection can be challenging. Malware can swiftly damage the system by doing pointless tasks that strain it and reduce its capacity to work efficiently. Both the traditional method and the behavior-based method can be used to identify malware. The traditional method relies on the malware's signature. The acts that the virus carries out while it is present on the computer, such as running operating system commands and downloading malicious files from the internet, define its behavior. The suggested approach locates the infection based on how it acts. Support vector machines and principal component analysis are both used in the study's proposed model. Our proposed model had an accuracy for genuine malware of Decision Tree 0.995, SVM 0.787, and Random 0.997.

Key words: Support vector machines , Analytical models , Computer viruses , Computational modeling , Malware

DOI: 10.1109/INOCON60754.2024.10512276

https://ieeexplore.ieee.org/abstract/document/10512276/authors#authors