World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:01, 2024

Fusion Models for Cyber Threat Defense: Integrating Clustering, Random Forests, and Support Vector Machines to Against Windows Malware

Authors : Azita Ramezani, Atousa Ramezani

Abstract : In the ever-escalating landscape of windows malware the necessity for pioneering defense strategies turns into undeniable this study introduces an avant-garde approach fusing the capabilities of clustering random forests and support vector machines SVM to combat the intricate web of cyber threats our fusion model triumphs with a staggering accuracy of 98.67 and an equally formidable f1 score of 98.68 a testament to its effectiveness in the realm of windows malware defense by deciphering the intricate patterns within malicious code our model not only raises the bar for detection precision but also redefines the paradigm of cybersecurity preparedness this breakthrough underscores the potential embedded in the fusion of diverse analytical methodologies and signals a paradigm shift in fortifying against the relentless evolution of windows malicious threats as we traverse through the dynamic cybersecurity terrain this research serves as a beacon illuminating the path toward a resilient future where innovative fusion models stand at the forefront of cyber threat defense.

Keywords : fusion models, cyber threat defense, windows malware, clustering, random forests, support vector machines (SVM), accuracy, f1-score, cybersecurity, malicious code detection
Conference Title : ICMLCS 2024 : International Conference on Machine Learning in Computer Security
Conference Location : New York, United States
Conference Dates : January 29-30, 2024