IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 2, December 2025

Impact Factor: 7.67

XRGuard: A Model-Agnostic Approach to Ransomware Detection Using Dynamic Analysis and Explainable AI

Ruday Kailas Gadekar, Om Gajanan Wakchaure, Akash Ravindra Dongare
Prof. J K Shimpi, Prof C V Patekar
Adsul Technical Campus, Chas, Ahilyanagar, Maharashtra, India

Abstract: *Ransomware remains a persistent and evolving cybersecurity threat, demanding advanced and adaptable detection strategies. Traditional methods often fall short as signature-based systems are easily circumvented by emerging ransomware variants, while techniques like obfuscation and polymorphism add complexity to the detection process. Although machine learning and deep learning techniques present viable solutions, the opacity of complex black-box models can hinder their application in critical security environments. This paper introduces XRGuard, a novel ransomware detection framework that utilizes machine learning techniques to analyze Event Tracing for Windows (ETW) logs, identifying critical file I/O patterns indicative of ransomware attacks. By incorporating XAI techniques such as SHapley Additive exPlanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME), XRGuard bridges the trust gap associated with complex machine learning models by providing transparent and interpretable explanations for its decisions. Experimental results demonstrate that XRGuard achieves a 99.69% accuracy rate with an exceptionally low false positive rate of 0.5%. By enhancing detection accuracy and offering clear explanations of its operations, XRGuard not only improves security but also fosters trust and a deeper understanding of ransomware behaviors.*

Keywords*:* Event tracing for windows (ETW), FileIO, machine learning, ransomware, XAI, explainable AI, SHAP, LIME

DOI: 10.48175/568