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 4, June 2025
Impact Factor: 7.67

# A Review on PDF Malware Detection: Toward Machine Learning Modeling with Explainability Analysis

**Prof. Shegar S. R[1]., Abhale Ritu Yogesh[2], Inamdar Alisha Akbar[2], Galande Sanika Bapurao[2]**
Assistant Professor, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2]
Samarth College of Engineering and Management, Belhe, Junnar, Pune Maharashtra, India

**Abstract:** *The "PDF Malware Detection: Toward Machine Learning Modeling with Explainability Analysis" project aims to develop a machine learning model to detect malware embedded within PDF files, focusing on enhancing both detection accuracy and transparency. By leveraging explainable AI techniques, the model seeks not only to identify malicious PDFs but also to provide insights into the decision-making process, offering a clear understanding of the features contributing to the detection of potential threats. This project combines cybersecurity and machine learning to improve the safety of digital documents in a user-comprehensible way.*

**Keywords:** PDF Malware Detection, Machine Learning Explainability Analysis , Feature Engineering Malicious PDF Analysis



DOI: 10.48175/IJARSCT-27683