iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** XI **Month of publication:** November 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.56514

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue XI Nov 2023- Available at www.ijraset.com*

# Malware Detection and Prevention Using ML

Neha Jadhav[1], Prof. Mrs. M. E. Sanap[2], Samiksha Katore[3], Srushti Mahadik[4], Akanksha Shendage[5]
*Computer Engineering SAE, Kondhwa*

***Abstract:*** ***The most prevalent issue on the internet today is malware. Due to its dynamic nature and ability to inherit characteristics from other types, polymorphic malware constantly modifies its properties to avoid being identified by traditional signature methodologies. The activity is carried out either at a certain moment or after a specific period of time. This study investigates machine learning model-based behavior-based detection techniques for detecting malware families and predict their presence through static or dynamic analysis.***
***Keywords: Support Vector Machine, Encrypted Traffic, Random Forest, and Malware Classification.***

## I. INTRODUCTION

This is now common place for people to use computers, smartphones, and the internet, and many people do so on a regular basis Malware prevention or anti-malware solutions can be designed with a unique signature to identify it, but malware detection and classification are crucial since they need to be done correctly to determine which family of malware the virus belongs to [1]. The current malware system incorporates signature-based and behavioral techniques into a typical antivirus detection workflow. Conventional malware detection techniques are not particularly good at detecting unfamiliar applications [2] .Such malware attacks are a severe and important problem as they can have a variety of harmful effects on the victim. Thus, early detection of viruses is critical to a computer system's security[4].

Instead of focusing on static signatures, malware researchers are now searching for more broad and scalable traits that can identify malware that was previously unknown. Static and dynamic analysis are the two fundamental methods used to analyze malware. While a program is performed in a real or virtual environment during dynamic analysis, the code and structure of a program are analyzed during static analysis without the program actually executing.

## II. LITERATURE SURVEY

*1) Study Of Malware Detection And Classification Using Ml*

In these research Soma Ghost uses one such machine learning methodology for malware detection. The antivirus programs were made to detect the presence of malicious software by comparing the information in the virus definitions, which is updated periodically. Static and dynamic options are combined together, and as a result, the integrated feature vector is used for machine learning-based teaching and categorization.

*2) Malware Analysis & Detection Using Machine Learning Algorithms*

In these research we studied that Akhtar , M.S. , Feng makes use of one such analysis of the virus. The present malware system uses behavioral and signature-based approaches as part of a standard antivirus detection method. Traditional methods of malware detection are not very effective and cannot detect software that is unknown. In recent years, machine learning has become a novel and challenging field in malware detection.

*3) Malware Detection Using Machine Learning Technique*

In these paper we learn that author M. S .Joshi has told that malware attacks are a major and important problem since they can have a variety of negative effects on the victim. Therefore, early virus detection is crucial to a computer system's security. The primary constraint is the time factor, which is crucial in the field of malware investigation since hundreds of systems may become infected every hour following the spread of a virus.

*4) On Malware Detection In The Android Operating System*

This research author Charles Badami presents a classifications of several Android malware detection techniques using static, dynamic, and family signature analysis. Furthermore, an analysis is conducted to determine the relative effectiveness of the indicated methods.

*5) Machine Learning Algorithm For Malware Detection*

This research author Nor Zakiah Gorment , Ali Selamat, Lim kok cheng studied that malware has become a persistent danger to cyber security, affecting computer systems, smart devices, and large-scale networks.

Thus we have studied the paper and design the system architecture diagram

## III. SYSTEM ARCHITECTURE

System Architecture for Machine Learning for Malware Detection and prevention

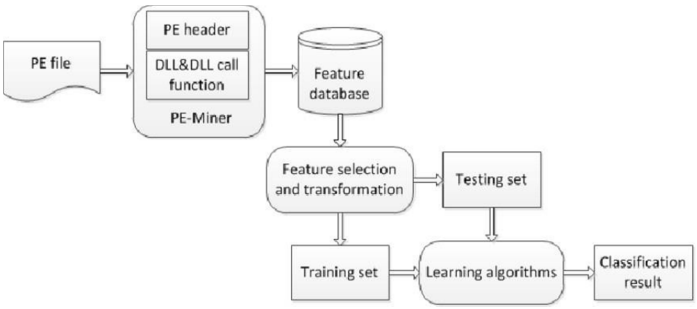



Fig. System Architecture for Malware Detection

The architecture of our malware detection system. The system consists of three main modules: (1) PE-Miner, (2) feature selection and data transformation, and (3) learning algorithms.

*1)* Module 1: PE-Miner parses PE tables of all executables to find out all PE header information, DLL names, and API functions inside each DLL as raw features;

*2)* Module 2: Information Gain value of each PE header, and calling frequency of each DLL and API function inside DLL are computed and those raw features with Information Gain values

*3)* Module 3: According to the features after PCA, transform every program in the database to its corresponding feature vector and then use a learning algorithm to derive a classification result from these labeled feature vectors

## IV. CONCLUSION

This paper is useful to Malware detection using machine learning to detect various viruses. In this paper, we explore the various different types of the modals which are used by various researchers in the malware detection**.**

## REFERENCES

[1] MalDAE: Detected as well as explained malware based on correlation and fusion of static and dynamic characteristics, (2019) 208-233, http : // dx. doi. Org /10.1016/j.cose.2019.02. 007 by W. Han, J. Xue, Y. Wang,L. Huang, and Z. Kong

[2] Malware classified using machine activity data and self-organizing feature maps by P. Burnap, R. French, F. Turner, and K. Jones https: // dx. doi. Org /1 0.1016/j.cose.2017.11.016, Computer Secure. 73 (2017) 399–410:

[3] F.D. Troia, C.A. Visaggio, T.H. Austin, M. Stamp,A. Damodaran J. Comput. Virol. Hacking Tech. (2017) 1–24,http://dx.doi.org/10.1007/s11416-015-0261–z, compares static, dynamic, and hybrid analysis for malware detection.

[4] A survey on forensic analysis of operating system logs, H. Studiawan, F. Sohel, and C. Payne, Digitalanalysis29(2019),120 ,https://dx.doi.org/10.1016/j.diin.2019.02.005,https://www.sciencedirect.com/science/article/pii/S1742287618303980.

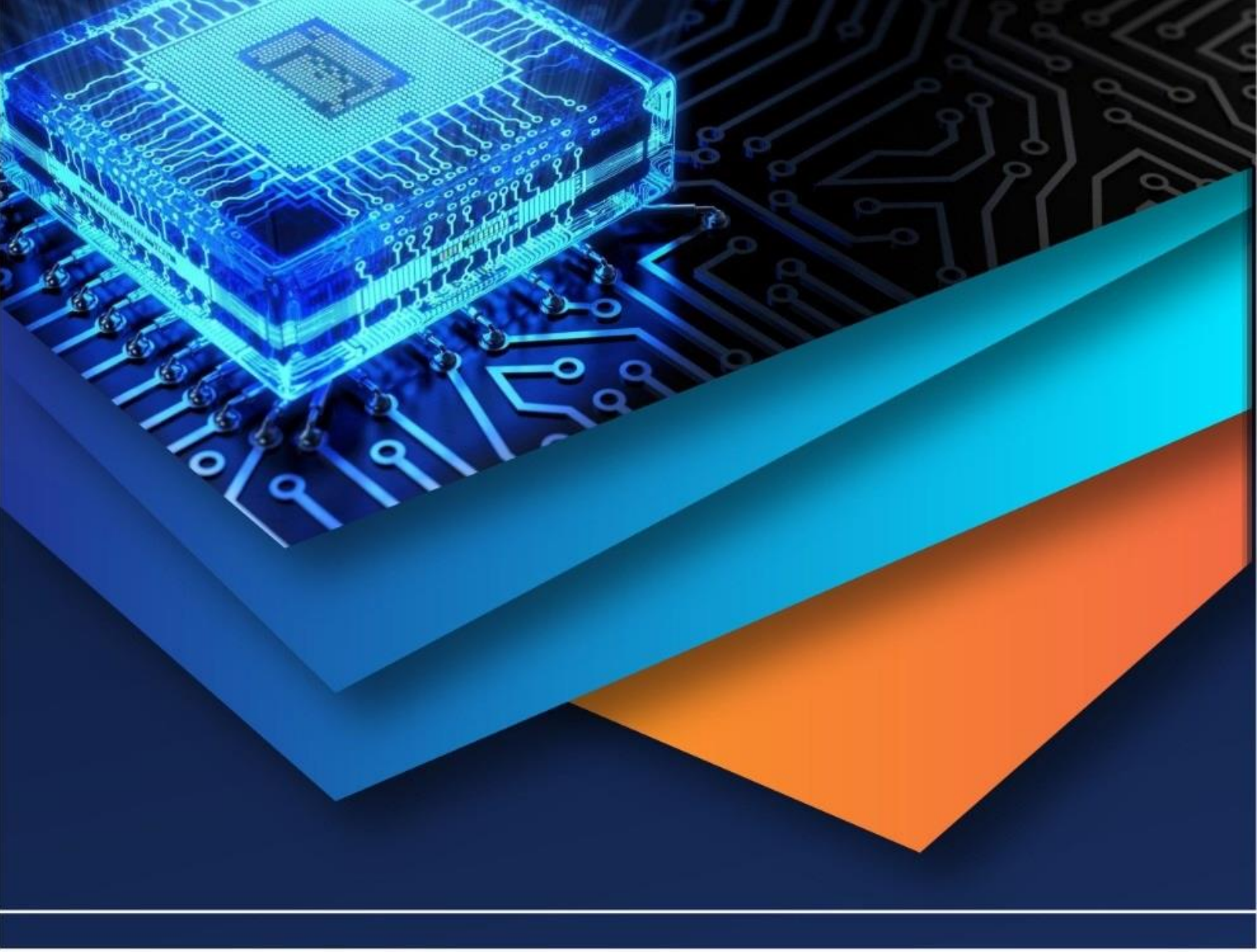
[5] S. Mahdavifar, A.A. Ghorbani, Application of deep learning to cybersecurity: A survey, Neurocomputing347 (2019) 149–176, http://dx.doi.org/ 10.1016/j.neucom.2019.02.056,http://www.sciencedire ct.com/science/article/ pii/S0925231219302954

[6] S. Alam, R. Horspool, I. Traore, I. Sogukpinar, made framework for metamorphic malware analysis and real- time analysis, Comput. Secur. 48 (2015) 212–233, http://dx.doi.org/10.1016/j.cose.2014.10.011,arXiv:arX iv:1011.1669v3,http://linkinghub.elsevier.com/retrieve/ pii/S0167404814001576.

[7] Khan, A. Mehmood, S. Khan, M.A. Khan, Z. Iqbal,W.K. Mashwani, A survey on intrusion detection and prevention in wireless ad - hoc networks, J. Syst. Archit. (2019)101701,http://dx.doi.org/10.1016/j.sysarc.2019. 101701

[8] K. Khan, A. Mehmood, S. Khan, M.A. Khan, Z. Iqbal, W.K. Mashwani, A survey on intrusion detection and prevention in wireless ad - hoc networks, J. Syst. Archit. (2019) 101701 ,http :// dx.d oi.org /10.1016/j.sysarc.2019.101701.

[9] R. Kaur, M. Singh, Hybrid real-time zero-day malware analysis and reporting system, Int. J. Inf. Technol. Comput. Sci. 8 (4) (2016)63–73,http://dx.doi.o rg/10 5815/ijitcs.2016.04.08,http://www.mecs-press.org/ijitcs/ijitcs-v8n4/v8n4-8.html.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY