GUJARAT TECHNOLOGICAL UNIVERSITY
(Established by Government of Gujarat under Gujarat Act No. : 20 of 2007)
ગુજરાત ટેક્નોલોજીકલ યુનિવર્સિટી
(ગુજરાત સરકારના ગુજરાત અધિનિયમ ક્રમાંક :૨૦/૨૦૦૭ દ્વારા સ્થાપિત)

Abstract of the Thesis

Name: **Amit Bhupendrabhai Parmar**

Enrollment No: **179999913001**

Faculty: **Computer Engineering**

Discipline/Branch: **Computer Engineering**

Title of the Thesis: "**Information Security against Malware Activities using AI Models"**

Abstract

Malware attacks are becoming increasingly difficult to detect using traditional methods because they constantly evolve and change their binary content. It makes it difficult for conventional signature-based detection systems to keep up. Machine learning (ML) approaches provide a promising answer to this issue. Malware-specific properties may be learned by training ML algorithms on an extensive collection of known malware samples. It allows them to detect new malware samples without known signatures. Two approaches have been proposed in the research work presented in the thesis. The first approach is the Performance Importance Weighted Random Forest (PERI-WRF) Learning model, which includes clustering and data reduction functions. The second approach is the Chimp-based malware detection, a unique based on machine learning (ML), YOLO Malicious Avoidance framework (CbYMAF). It includes three main stages: classification, preprocessing, and feature extraction. The preprocessing states noise to be removed and then redundancy from a dataset. In the feature extraction step, characteristics of the malware samples, such as memory and hypervisor characteristics, are extracted. The feature selection phase eliminates irrelevant features from the extracted group. The classification phase uses a YOLOv3 object detection algorithm to classify the PE malware samples. YOLOv3 is a fast and accurate object detection algorithm that may be applied to real-time malware sample detection. These results show that the PERI-WRF method and CbYMAF are highly effective malware detection systems. It produces few false positives and a high accuracy for detecting new malware strains. We also evaluated the robustness of CbYMAF to evasion attacks. We conducted a series of evasion attacks, such as code obfuscation and polymorphism, and found that

CbYMAF could see them even after the malware samples were avoided. These results show that the PERI-WRF method and CbYMAF are robust mechanisms for detecting malware samples even after evading them. The PERI-WRF method and CbYMAF can potentially be new approaches to finding malware. It is a technique that may be applied to protect computer systems from malicious assaults and is incredibly effective and reliable.

This PhD thesis would be helpful in improving performance of Anti malware systems by applying AI techniques.

List of Publication(s):

1. Amit Parmar, Dr. Keyur N Brahmbhatt "Effectiveness of the Static Analysis using PE files for Malware Detection", Solid State Technology, Volume: 63 Issue: 6, 2020.

2. Amit Parmar, Dr. Keyur N Brahmbhatt "A NOVEL MALWARE DETECTION APPROACH USING PERFORMANCE IMPORTANCE WEIGHTED RANDOM FOREST (PERI-WRF) LEARNING MODEL", Indian Journal of Computer Science and Engineering (IJCSE), e-ISSN : 0976-5166, p-ISSN : 2231-3850, Vol. 13 No. 5 Sep-Oct 2022.

3. Amit Parmar, Dr. Keyur N Brahmbhatt "An Optimized Intelligent Malware Detection Framework for Securing Digital Data", Wireless Personal Communications, Volume 133, Dec-2023. (Scopus Indexed - UGC CARE Group-II)