IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

ROBUST INTELLIGENT MALWARE DETECTION USING DEEP LEARING AND MACHINE LEARNING

[1]K. DILEEP KUMAR, [2]G. PRAVEENA, [3]S. BINDU, [4]S. B SRIDHARANI, [5]P. KUSHWANTH KALYAN

[1]Student, [2] Student, [3] Student, [4] Student, [5] Student
COMPUTER SCIENCE & ENGINEERING

VISAKHA INSTITUTE OF ENGINEERING & TECHNOLOGY
VISAKHAPATNAM, ANDHRA PRADESH
INDIA

Under Guidance of
K. PRASANNA LATHA
Visakha Institute of Engineering & Technology
Faculty of Computer Science Engineering
Visakhapatnam, Andhra Pradesh

Under Guidance of
A.S.C. TEJASWINI KONE
Visakha Institute of Engineering & Technology
HOD of Computer Science Engineering
Visakhapatnam, Andhra Pradesh

Abstract: Malware remains a significant security concern in today's digital landscape, with traditional detection methods often proving ineffective against evolving threats. Recent approaches leverage machine learning algorithms, particularly deep learning, to analyze malware effectively. However, existing research is often biased due to training data limitations. To address this, this study evaluates classical machine learning and deep learning models for malware detection using diverse datasets. A novel image processing technique is also proposed to enhance detection accuracy. Results show deep learning outperforming traditional methods, paving the way for scalable and real-time malware detection systems.

INTRODUCTION

This project is titled "Robust Intelligent Malware Detection Using Deep Learning". It will develop a deep learning-based malware detection system that is more robust and intelligent than traditional methods. The system will be able to detect malware with a high degree of accuracy, even in cases where the malware has been obfuscated or modified. The purpose of the project is to develop a malware detection system that can help to protect computer systems from malware attacks.

The system will be used by businesses, governments, and individuals to protect their data and systems from malicious software. Deep learning is making crucial advances in solving Problems that have restricted the best attempts of the artificial intelligence community for many years. It has proven to be excellent at revealing complex structures in high-dimensional data and is therefore applicable to lots of domains of science, business and Government The main features of this project are that this project encompasses its malware detection capabilities, encompassing both static and dynamic analysis.

The system excels in pinpointing malware tailored to specific systems or applications, showcasing its adaptability and precision. It boasts an exceptional ability to identify obfuscated or altered malware, demonstrating its resilience against evolving threats. Moreover, the system goes beyond mere detection, offering users in-depth insights into the malware
it encounters.

NEED OF THE STUDY

The study on "Robust Intelligent Malware Detection Using Deep Learning" is imperative in today's cybersecurity landscape due to the escalating complexity and sophistication of cyber threats. Traditional malware detection methods struggle to keep pace with the evolving tactics of malicious actors who employ obfuscation techniques to evade detection. This project aims to bridge the gap by leveraging deep learning, a powerful technology capable of analysing complex patterns in high-dimensional data. By harnessing the capabilities of deep learning, the system will enhance malware detection accuracy, even in cases of obfuscated or modified malware. This is crucial for businesses, governments, and individuals who rely on robust cybersecurity measures to safeguard their sensitive data and systems from malicious software.

Furthermore, the study addresses the need for real-time detection and insightful analysis of malware behaviour. In today's interconnected world, the speed of detection is paramount to mitigate the impact of cyber-attacks. Deep learning-based systems offer the potential to analyse dynamic malware behaviour patterns, providing valuable insights into the nature, origins, and potential impact of detected malware. By offering in-depth analysis capabilities, the system empowers users with actionable intelligence to proactively defend against cyber threats. Moreover, its adaptability and precision in pinpointing malware tailored to specific systems or applications showcase its resilience against evolving threats, making it a crucial asset in the fight against cybercrime.

OBJECTIVE

Robust Intelligent Malware Detection Using Deep Learning and Machine Learning" is to develop an advanced malware detection system that combines the strengths of deep learning and traditional machine learning. This system aims to achieve robust intelligence, enhancing its ability to accurately identify and classify malware even when faced with obfuscation or modification. The goal is to provide a more effective and resilient solution against evolving cyber threats in the digital environment

Fig. 1 – Roles For This Project

HARDWARE

The hardware company developing "Robust Intelligent Malware Detection Using Deep Learning and Machine Learning" might be called "Secure Tech Innovations" or "Cyber Defense Systems." These names suggest a focus on security technology and the development of innovative hardware solutions for robust malware detection using advanced techniques like deep learning and machine learning are as follows

1. Processor: Pentium IV or higher
2. RAM: 256 MB
3. Space on Hard Disk: minimum 512MB

these are hardware needs to complete this Project

SOFTWARE

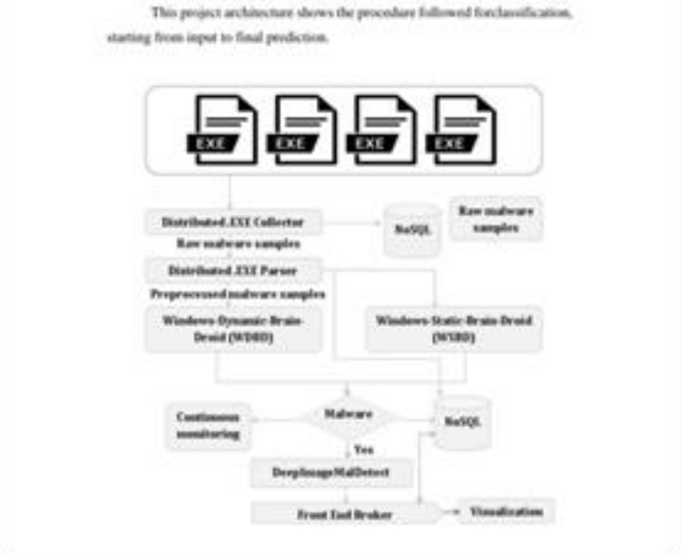
The software company developing "Robust Intelligent Malware Detection Using Deep Learning and Machine Learning" could be named something like "Cyber Shield Technologies" or "Intelligence Solutions." These names convey a focus on cybersecurity and the development of intelligent solutions for malware detection using advanced techniques like deep learning and machine learning.

1. Python
2. Django
3. MySQL
4. WampServer

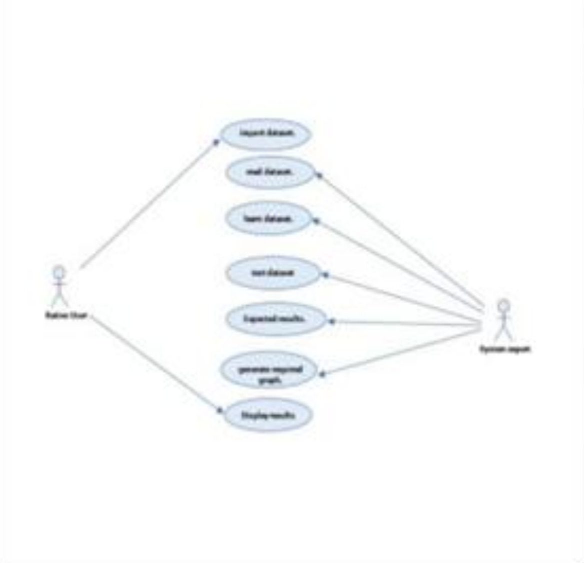
These are the software components to complete this and make Prototype of over Project.

PROJECT ARCHITECTURE

This project architecture shows the procedure followed for classification, starting from input to final prediction.

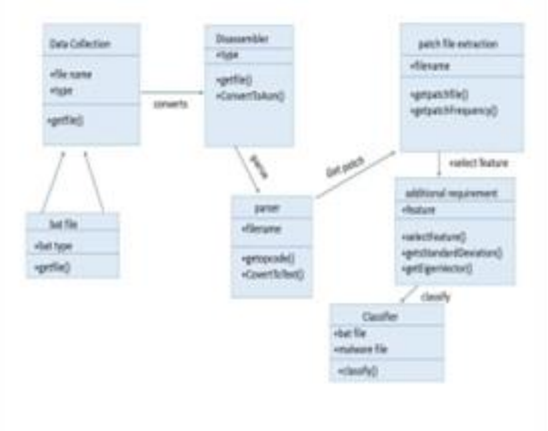

This project architecture shows the procedure followed forclassification,
starting from input to final prediction.
EXE
EXE
EXE
EXE
Distributed .EXE Collector
Raw malware samples
NoSQL
Raw malware samples
Distributed .EXE Parser
Preprocessed malware samples
Windows Dynamic Brain-Droid (WDBD)
Windows Static Brain-Droid (WSBD)
Continuous monitoring
Malware
NoSQL
Yes
DeepImageMalDetect
Front End Broker
Visualization

USE CASE



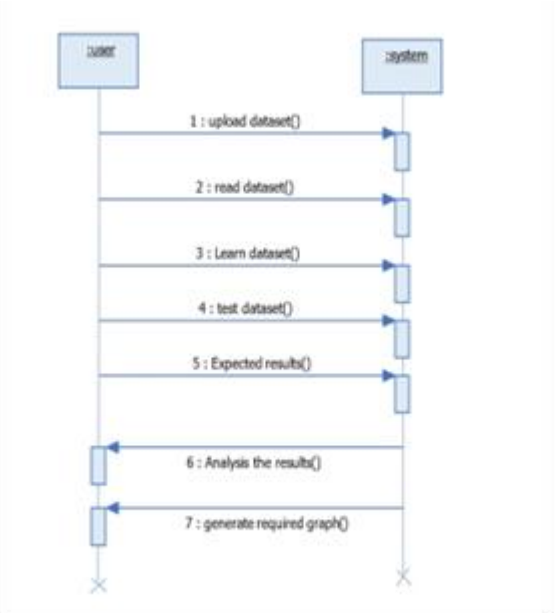
CLASS DIAGRAMS

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



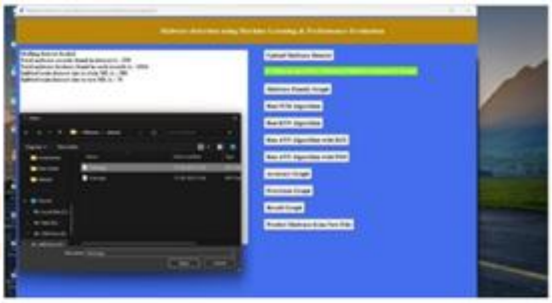
SEQUENCE DIAGRAM

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart

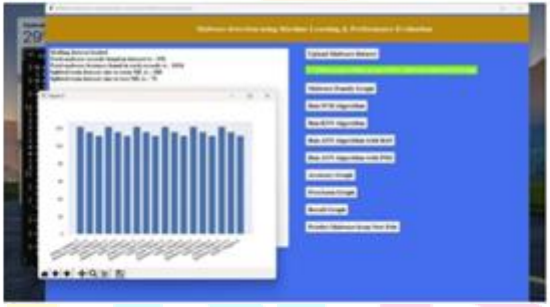


IMPLEMENTATION PROCESS

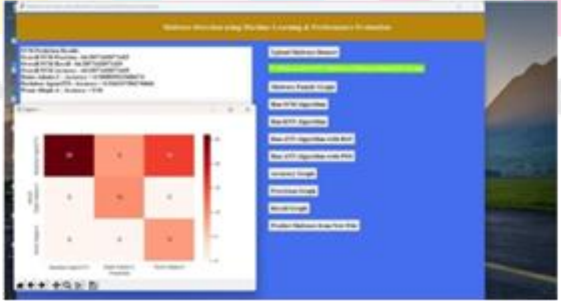
Step 1: Run Program and Upload Dataset.



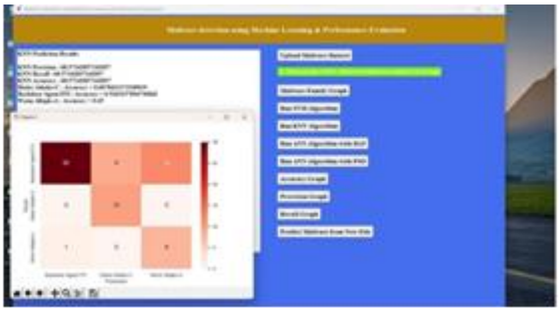
Step 2: Click on malware family graphs.



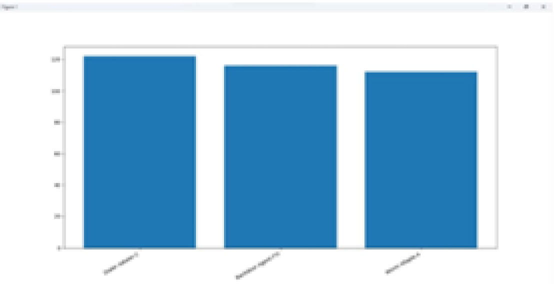
Step 3: Click on Run SVM Algorithm.



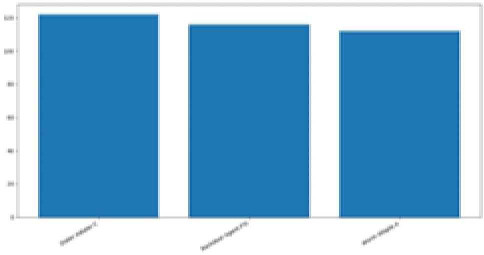
Step 4: Click on Run KNN Algorithm



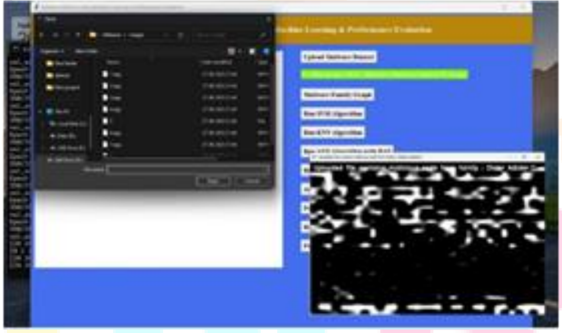
Step 5: Click on Accuracy Graph.



Step 6: Click on Precision Graph.



Step 7: Click on Predict Malware from New File.



CONCLUSION

Deep learning is an awesome way to detect malware with precision. It can detect both familiar and unfamiliar threats, plus it can recognize patterns in the data that we might not catch with a human eye. Deep learning might have some limitations and can give off false positives, but it's still a great choice for detecting malicious activity. Definitely worth considering when creating a security plan. This project proposed an efficient malware detection and designed a highly scalable framework to detect, classify and categorize zero-day malwares. This framework applies neural network on the collected malware from end user hosts and follows a two-stage process for malware analysis. first stage, a hybrid of static and dynamic analysis was applied for malware classification. In the second stage, malware was grouped into corresponding malware categories using image processing approaches. Various experimental analysis conducted by applying variations in the

models on publicly available benchmark dataset and indicated the proposed model outperformed classical MLAs. The developed framework can analyze large number of malwares in real-time and scaled out to analyze even larger number of malwares by stacking a few more layers to the existing architectures.

REFERENCES

1. https://ieeexplore.ieee.org/document/9850588/
2. https://ieeexplore.ieee.org/document/9793102/
3. https://ieeexplore.ieee.org/document/9368268/
4. https://ieeexplore.ieee.org/document/10374768/
5. https://ieeexplore.ieee.org/document/9061419/
6. https://ieeexplore.ieee.org/document/9703021/
7. https://ieeexplore.ieee.org/document/9573991/
8. https://ieeexplore.ieee.org/document/10150836/
9. https://ieeexplore.ieee.org/document/10073874/
10. https://ieeexplore.ieee.org/document/9467300/
11. https://ieeexplore.ieee.org/document/8596348/
12. https://ieeexplore.ieee.org/document/10151567/

DOCUMENTATION LINK:
https://docs.google.com/document/d/13Xb8kCUErbWRDbao9Op1Fg0GMWaf4vpx/edit?usp=drivesdk&ouid=102709497652126547364&rtpof=true&sd=true

CODE LINK:
https://github.com/DileepKammila/ROBUST-INTELLIGENT-MALWARE-DETECTION-USING-DEEP-LEARING-AND-MACHINE-LEARNING