1 INTRODUCTION

1.1 Overview

The process of dissecting malware to understand how it works, determine its functionality, origin and potential impact is called malware analysis. With the millions of new malicious programs in the wild, and the mutated versions of previously detected programs, total malware encountered by security analysts has been growing over the past years.[4] Consequently, malware analysis is critical to any business and infrastructure that responds to security incidents.

1.2 Purpose

In order to identify malicious internet activity,the tools check whether the suspicious item is coming from a bad url or c2 channels.the tools verify suspicious links against security data collected from miilons of devices worldwide and that is how they offer protection against known and unknown threats

2 LITERATURE SURVEY

2.1 Existing problem

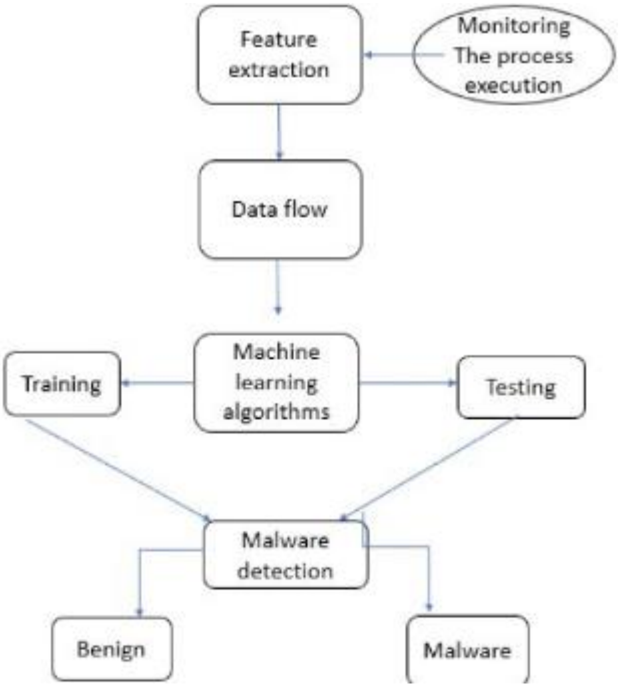
Malware infiltrates systems physically, via email or over the internet. Phishing, which involves email that appears legitimate but contains malicious links or attachments, is one of the most common malware attack vectors. Malware can also get onto devices and networks via infected USB drives, unpatched or fraudulent software and applications, insider threats, and vulnerable or misconfigured devices and software.

2.2 Proposed solution

1. Identify various attack scenarios for the study that will assist in the feature selection process
2. Using machine learning methods to predict malware attacks and build a classifier to automatically detect and label an event as "Has Detection or No Detection".
3. ML assist in recognizing attack patterns using datasets of previous attacks to predict future attacks trends and responses.

3 THEORITICAL ANALYSIS

3.1Block diagram



3.2Hardware / Software designing

➢ Machine learning

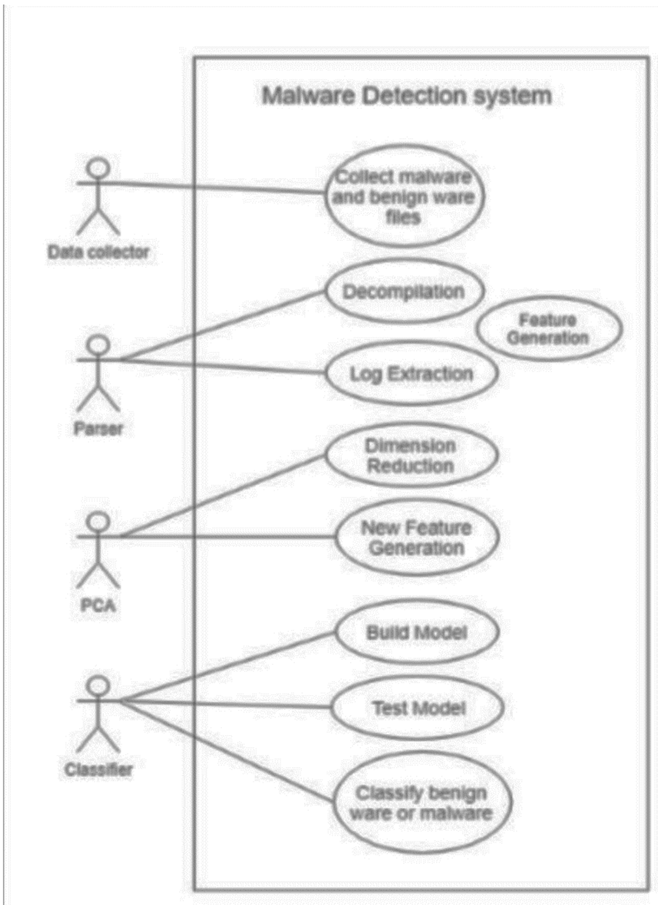
➢ Python

➢ Google Collab

4 ·EXPERIMENTAL INVESTIGATIONS

➢Dynamic malware analysis and detection tools provide an environment that executes the malware and observes its behavior. Malicious file creation, register changes, or malicious network activity can be logged and made ready to analyze for the malware analyst.

5 FLOWCHART



5 RESULT

Malware Detection Rate versus Complexity of Malware.

Test results indicate that when the complexity of malware increases, it becomes more difficult to detect the malware (Fig. 4). This is because recently, malware authors started to use some new techniques such as packing, obfuscation, and code encryption to hide the malware from anti-malware tools.

6 ADVANTAGES &DISADVANTAGES :

Advantages: fast and safe .low resource. consumption. multipath malware analysis.more secure than dynamic analysis .high accuracy

Disadvantages: can’t analyse obfuscated and encryption malware.can’t detect unknown malware

7 APPLICATIONS :

As such,many anti-malware software vendors such as symantac,Avast,eset,bitdefender developed different malware detection techiques

8 CONCLUSION

This research has proposed a methodology to learn well-known malware analysis and detection tools and compare the performance of these tools on existing and unknown malware. Test results have shown that it is almost impossible to detect malware by only using one tool. However, by using a combination of tools, the detection rate was improved immensely: 84% DR and 87.5% ACY.

9 FUTURE SCOPE

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information

10 BIBILOGRAPHY

1. https://www.kaggle.com/code/kishorejughead/malware-detection-with-rf/edit