Detecting Malware Applications Using Machine Learning

MANOJ SIRIGIRI
Department of Computer Science and Engineering Sathyabama Institute of Science and Technology Chennai, India
(student)
manojsirigiri@gmail.com

R. YOGITHA
Department of Computer Science and Engineering Sathyabama Institute of Science and Technology Chennai, India
(assistant professor)
yogitha.cse@sathyabama.ac.in

R. AISHWARYA
Department of Computer Science and Engineering Sathyabama Institute of Science and Technology Chennai, Ind
(assistant professor)
aishwarya.cse@sathyabama.ac.in

Abstract— **Online privacy for people is getting worse every day. Computer malware is tainting the data records of some well-known companies. Viruses that infect computers are becoming more sophisticated. Hackers can gain access to a network and change data once inside. This article discusses several types of malware and communication strategies, such as Trojans, keyloggers, port forwarding, source code obfuscation, application format converters, and social engineering. Cyberattack defenses such as pre- and post-installation detection assist in determining the need for cybersecurity.**

Keywords— Computer malwares, Trojan, Keyloggers, Port forwarding, social engineering, Pre installation detection, Post installation detection

I. INTRODUCTION

Malware, often known as malicious software, is a general word for programs or applications that are intended to harm or infect electronic devices. Your device might be held hostage, have important and private information stolen from it, or have malicious software installed that watches your internet activity. All kinds of electronic gadgets, including smartphones, laptops, tablets, smart TVs, and even game consoles, are susceptible to malware infection. Malware often reproduces itself in order to spread. The virus can continue to function unnoticed inside the device's files as long as it is executing that file. Malware might be inactive and wait for a file to be opened before it begins to function and do damage. Once activated, malware might spread. First of all, malware is a term used to describe malevolent practices designed by software programmers with the purpose of harming a computer or server. The virus can corrupt a target's computer after being implemented or otherwise introduced into the target's machine. In olden times, malware used to be simply detected using many anti-virus applications due to a lack of proper code hiding and social engineering techniques, but now that these things have gotten more advanced, they have started to cause more damage to the victims. People being more involved in the internet gives cyber criminals a better chance to lure more people into their trap. The evolution of malware increased rapidly, which gave a better challenge to the modern malware protection system. The capacity to fend off and recover from cyberattacks can be referred to as "cybersecurity. The National Institute of Standards and Technology describes cybersecurity as the capacity to protect or safeguard the use of cyberspace against threats. A software program known as an antivirus program guards against viruses on your PC, laptop, phone, or other internet-connected device. Antivirus software plays a significant part in cyber security. The primary role of virus scanners is to protect your computer against malicious programs and other malware. It achieves this by evaluating each threat it encounters to a "blacklist." This list includes each malware that the security software is knowledgeable of. Antivirus detects malware that has already been installed on a machine (post-installation detection) using various methods of scanning based on the user's interest. Machine learning is an area of computing algorithms that is rapidly expanding and aims to mimic human intelligence by learning from its past and its surroundings. Applications utilize machine learning algorithms to respond adequately to cyberattacks. Huge data sets of potential attacks will be analyzed in order to determine patterns and the physical features of applications and their malicious behavior and assist with this. When comparable events are found, machine learning comes into action so that the trained model can distinguish them into malware and a safe one.

II. Literature review

The history of cyberattacks and their prevention attacks should be known to one who wants to deal with advanced malware. This section contains some related work regarding my research. **Yalin, Y., & Haodan, R et.al [1]**. In this paper the characteristics and principles of trojans are analyzed and the detection methods are compared. This paper includes detection methods like Sand box testing and Heuristic based testing. **Al-Asli, M., & Ghaleb et.al [2]**. This paper shares previous work on malware detection using signature-based algorithms. Cybercrime investigation models are being combined with existing antivirus software in order to extend their benefits to the society. **Aslan et.al [3].** This paper briefs different malware detection techniques Evolution of malware detection and history of malware discussed in this paper. **Idka et.al [4].** In this study, they addressed what malware is and the many varieties of malware. Future malware dangers and techniques are covered in this study. Paper includes future malware threats and techniques. **Asish, M. S., & Aishwarya, R. et.al [5]**. In many aspects, this study described several hacking tactics and countermeasures. Learned about different types of malwares and after effects of the installation of those malware. Discussed all kinds of malware form old to new to describe the evolution of malware. Explained how traditional defense mechanisms (such as signature-based malware identification) utilized by antivirus would struggle to meet the difficulties of modern malware. **Rathore et.al [6]**. Malware analysis and detection have been modelled as machine learning and deep learning problems in this paper. They constructed these models using practices (cross-validation, correcting class imbalance issue, etc.). **Namanya et.al [7]**. To provide background knowledge for the intended study on developing malware detection systems, this study provides an overview of the malware world. The fundamental knowledge of ransomware and anti-malware programs is reviewed in this study. They provided abstracts of articles about the development of malware, malware analytical techniques, virus evasion tactics, and currently used malware detection approaches. **Bhardwaj et.al [8]**. Explained the destruction caused by keyloggers in past and how advance they became. Keyloggers aka silent cyber weapon is deadly and undetectable in most cases. Described the economic damage caused by keyloggers. Keyloggers function at a higher privilege level than ordinary malware, making them extremely difficult to identify and eliminate. **Parthy et.al [9]**. This document categorizes numerous social engineering assaults based on the perpetrator's perspective. Explained about all types of enterprise attacks and classified them. Many new social engineering techniques were discussed likes reverse social engineering. This paper will assist the reader understand how social engineering could be used opposed to businesses. **Kunwar et.al [10]**. This article delves into the threats, security concerns, and many sorts of social media cyberattacks. Discussed many thigs about spam and malicious ads in social media. Found detailed information about the number of users who uses social media and how many are lured into these cyber-attacks gave a clear ratio about much more information.

III. TYPES OF MALWARES AND METHODOLOGIES

A. Trojan

By using social engineering, Trojans are tricked into running on users' computers. Once a Trojan has been loaded, hackers can use it to monitor victims, steal their personal data, and acquire remote access with a back door to the targets' systems. The activities could include tampering with the victim's data, monitoring targets actions such as spying on target displays, and so on.

For instance, the most dangerous and widely used Trojan is known as 888 Remote Access. This Trojan allows attackers to violate victims' privacy by doing various things, like gaining access to secret information by monitoring user activities with built-in keyloggers. Display monitoring allows attackers to see the live feed of what victims are seeing on their screens. attacker can see his targets using a system's webcam in real time. Spreading viruses and other malware by obtaining complete control over the browser, CMD, and file management, drive formatting, and deleting, downloading, or modifying files and file systems. Remote Trojrans are typically hidden within a user's requested program, for example a game, or delivered as an e - mail attachment. This directly runs encoded malicious code to give the administrator control over the application.

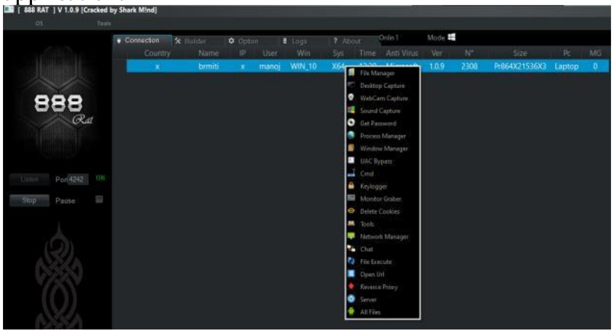


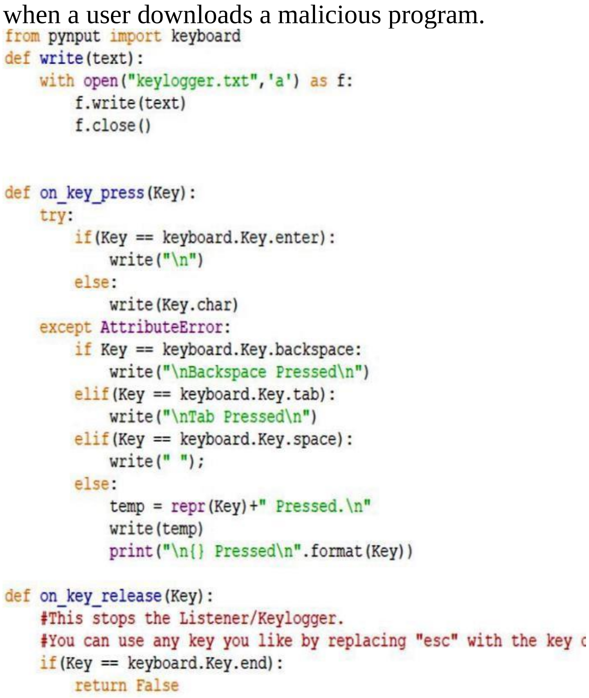
Figure 1: trojan interface

B. Keylogger

The Keystroke logger software, sometimes known as keyloggers, is a category of malware that has the ability to covertly track keyboard input from users in order to steal important information. Thus, keyloggers pose a serious risk to both personal and professional activities including payments, internet banking, mail, and small talk are all available. The keyboard is the main target. due to the fact that it is the most common method for users to connect with computers and because it makes it possible for keyloggers to collect user input from the system. Software keyloggers and handset keyloggers are the two types of keyloggers available today.

Software keyloggers are much more prevalent, easier to set up, and more likely to do significant damage. Keyloggers do two tasks: they guide into the customer input stream to record keystrokes and they communicate the data to a distant place (mail). A common hardware keylogger records keystrokes using a physical circuit that is located between both the keyboard and the machine. It stores a record of every keystroke on the keyboard in internal memory, which may be retrieved by keying in a sequence of characteristics that have been predefined. They are frequently designed to appear innocent and to mix in with the other equipment or cables. They may also be added or modified to a keyboard's internal circuitry, or the keyboard may be designed with this functionality.

Software keyloggers are programs that need to be installed on a computer to collect keystroke data. They are the most typical technique used by hackers to obtain user keystrokes. A keylogger application is already installed on a computer when a user downloads a malicious program.



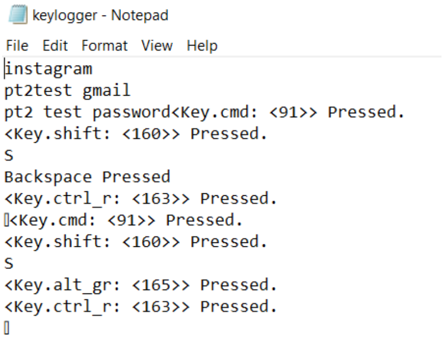
```
from pynput import keyboard
def write(text):
    with open("keylogger.txt",'a') as f:
        f.write(text)
        f.close()


def on_key_press(Key):
    try:
        if(Key == keyboard.Key.enter):
            write("\n")
        else:
            write(Key.char)
    except AttributeError:
        if Key == keyboard.Key.backspace:
            write("\nBackspace Pressed\n")
        elif(Key == keyboard.Key.tab):
            write("\nTab Pressed\n")
        elif(Key == keyboard.Key.space):
            write(" ");
        else:
            temp = repr(Key)+" Pressed.\n"
            write(temp)
            print("\n{} Pressed\n".format(Key))

def on_key_release(Key):
    #This stops the Listener/Keylogger.
    #You can use any key you like by replacing "esc" with the key c
    if(Key == keyboard.Key.end):
        return False
```

Figure 2: keylogger source code

The software which could operate like a basic keylogger to obtain all user data from clients by recording them keyboard strokes and mouse actions without revealing the clients' names. As a result, the client is unaware of what is going on in the foundation. The application can keep track of information, save it in a specific location and email it to the owner if needed. The program will conceal itself from the operating system while it is running in the background. I recognize that the bar for monitoring data and collecting it either for legal or illegal purposes has been greatly raised by this technique.

Figure 3: user typing confidential information

After being installed, the keylogger records each keystroke you make on the operating system you're using and looks at the routes they travel. This enables a keylogger piece of software to keep track of and log every keystroke you make.



```
instagram
pt2test gmail
pt2 test password<Key.cmd: <91>> Pressed.
<Key.shift: <160>> Pressed.
S
Backspace Pressed
<Key.ctrl_r: <163>> Pressed.
▯<Key.cmd: <91>> Pressed.
<Key.shift: <160>> Pressed.
S
<Key.alt_gr: <165>> Pressed.
<Key.ctrl_r: <163>> Pressed.
▯
```

Figure 4: keystrokes recorded

C. Backdoor

Any method by which permitted or not permitted users may get around common security controls and get high-level access rights on a group of computers or software applications is referred to as a backdoor. Once inside, fraudsters could use a backdoor to take control of equipment, install further malware, and steal financial and personal data. If both the target and the attacker are on the same network, a back door can be easily opened. Otherwise, the attacker employs port mapping to establish an unattended communication bridge between the attacker's and the target's systems. Back doors enable attackers to re-enter the victim's network at any time.

D. Port Forwarding

If the victim's computer is not linked to his local network, the attacker utilizes port forwarding to gain access to it. Computers or services on private networks can connect with other publicly or privately accessible computers or services on the internet thanks to port forwarding, also known as port mapping. The goal of port forwarding is to establish a connection between a router's public, WAN, and secret LAN, Internet protocol addresses for a device on that secure network. Several software's and applications can be used for port forwarding like port map.io. port forwarding is just like call forwarding.

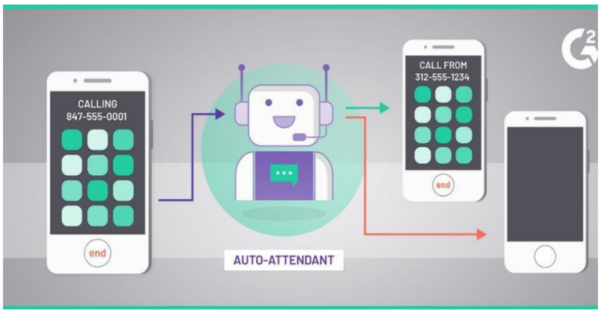
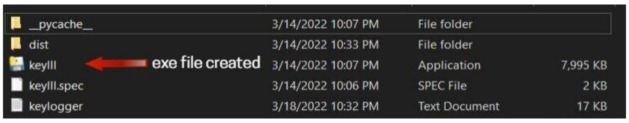


Figure 5: port forwarding

E. Malware Formatting

Malware comes in a variety of formats, including EXE, PDF, zip, and JPEG files. These file types make it simple for hackers to distribute malware or other harmful software via numerous social media platforms and mail file formats. assists attackers in hiding their source code and renders them invisible to various antivirus software. Several software's are present to change a piece of code into a specific format like null soft script. Changed python keylogger script into an exe file for source code hiding and better malware delivery.



```
_pycache_                          3/14/2022 10:07 PM   File folder
dist                               3/14/2022 10:33 PM   File folder
keylll      exe file created       3/14/2022 10:07 PM   Application      7,995 KB
keylll.spec                        3/14/2022 10:06 PM   SPEC File            2 KB
keylogger                          3/18/2022 10:32 PM   Text Document       17 KB
```

Figure 6: file formatting

D. Social Engineering

An extensive range of malicious acts carried out via interactions with other individuals are referred to as "social engineering." Users are psychologically manipulated into disclosing important data or committing security blunders. A payload can be sent to a target in a variety of formats by an attacker.

- Exe (commonly found in third-party applications and mod applications; by creating a cracked version of a paid software and encoding it with a payload, users will easily install them because they are free and simple to install, but they will overlook their security.)
- HTML format (in the name of cookies, it is possible to hack into victims' devices)
- Chrome extensions
- Jpg (photo format) (Photo has been tainted with malicious code. The code will be executed if you click on it.)
- PDFs containing malicious code Opening it will cause the code to run.

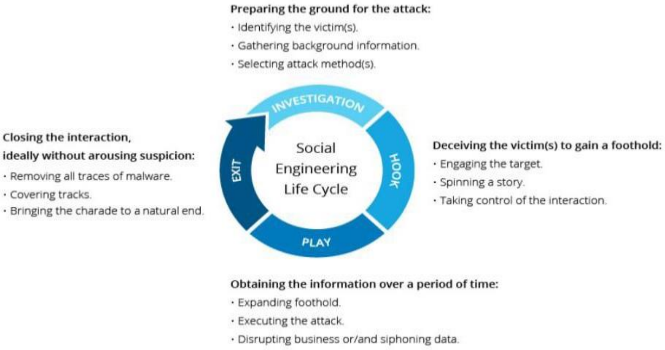

Preparing the ground for the attack:
• Identifying the victim(s).
• Gathering background information.
• Selecting attack method(s).
INVESTIGATION
Social Engineering Life Cycle
HOOK
PLAY
EXIT
Deceiving the victim(s) to gain a foothold:
• Engaging the target.
• Spinning a story.
• Taking control of the interaction.
Obtaining the information over a period of time:
• Expanding foothold.
• Executing the attack.
• Disrupting business or/and siphoning data.
Closing the interaction, ideally without arousing suspicion:
• Removing all traces of malware.
• Covering tracks.
• Bringing the charade to a natural end.

Figure 7: social engineering

IV. Post installation detection

post installation detection is an application or software detecting Malware malicious applications using the data post installation detection is an application of the software detecting Marlboro malicious applications using the data.

A. Anti-Virus

Antivirus program is a sort of application that is used to protect against, detect, and eradicate malware from a machine. After installation, most antivirus program run on autopilot to provide real-time protection against viral threats. Effective malware protection systems can also include extra security capabilities such as configurable firewalls and Traffic shaping to protect both data and hardware from infections like as worms, Trojans and adware. Antivirus software begins to function by evaluating the data and apps on the machine to a database containing known malware types. It will also analyze PCs for any possible threats from novel or unidentified malware kinds because hackers are always creating and disseminating new malware. Heuristic detection, generic detection, and specific detection are the three detection techniques used by the majority of programs. A malware file is normally isolated and/or marked for removal by the application when it is discovered, reducing the risk to your device and making the file unusable. Traditional antivirus program aren't as effective at thwarting threats on their own as they should be. These factors have led to the adoption of methodologies by many antivirus software vendors today, including global scanning, human threat analysis, industry collaboration, and cloud integration.

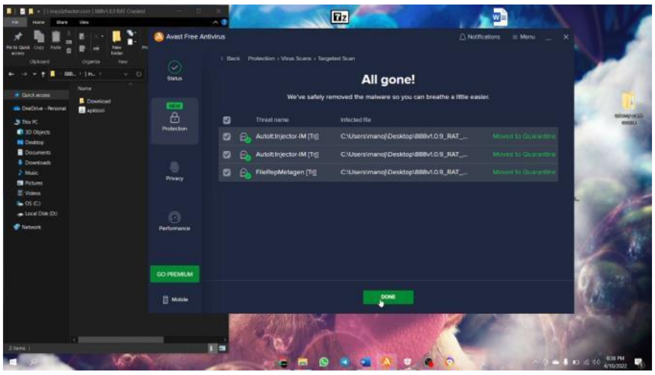
B. Types of anti-virus detection

Malware is computer software that was purposefully created to enter or harm a computer without the owner's permission. This contains, among other things, Trojan horses, worms, and viruses. Malware detection is the process of identifying whether a certain application is harmful or benign or of identifying the presence of viruses on a host system.

- **Signature-based detection**: Every reliable piece of software has a digital signature. A binary pattern is all that a signature is. When a file is scanned by an antivirus tool, its signature is evaluated and compared with a vast database of digital signatures. The antivirus will immediately alert you if it has a history of being harmful.
- **Heuristic based detection**: To identify the contamination status of your file or program, code behavior and patterns will be examined. Any suspicious code is executed in a virtual environment during runtime to further test it. You can use this strategy to find new viruses that haven't yet been uploaded to the antivirus databases.
- **Behavioral-Based Detection**: Your antivirus software is constantly scanning your computer. If one of your software starts behaving strangely, doing serious harm and requesting more read and write permissions, your antivirus will detect this and notify you.
- **Sand box detection**: If your antivirus software is unsure if a program or file is infected with malware and suspects it, it will execute it in a sandbox environment. This detection will run your software in a virtual system to examine how it acts. Examining system failures examining startup applications to see if they are consuming excessive amounts of RAM and network bandwidth.

C. Types of scans in antivirus:

- **On access scanning:** This scanning begins when the antivirus program is launched Real-Time Scanning, sometimes referred to as On-Access Scanning, is the process where your security program continuously scans the data that users access while using your machine.
- **Manual scanning:** Manual scanning allows you to start a malware scan whenever you want.
- **Scheduled scanning:** Some software lets you schedule scans for specified days or weeks These are an essential component of maintaining your system's integrity. They carefully scan your devices for malware and many other dangers on a regular basis.



All gone!

We've safely removed the malware so you can breathe a little easier.

Threat name	Infected file	
AutoIt:Injector-IM [Trj]	C:\Users\manoj\Desktop\888v1.0.9_RAT_...	Moved to Quarantine
AutoIt:Injector-IM [Trj]	C:\Users\manoj\Desktop\888v1.0.9_RAT_...	Moved to Quarantine
FileRepMetagen [Trj]	C:\Users\manoj\Desktop\888v1.0.9_RAT_...	Moved to Quarantine

Figure 8: working of antivirus

- **Quick scans:** Quick scans look at frequently used areas of a system like temporary files, the OS directory, and computer cache memory.

IV. PRE-INSTALLATION DETETCTION

Preinstallation data is that any information you can provide about a file without actually running it. Among other related data, this could comprise descriptions of the executable file format, the actions of the application, code descriptions, statistics for binary data, text strings, and information obtained through code emulation. The information collected can help us distinguish whether a download is malicious or not by training a machine learning model on the same. The model can help us understand the probability of a particular file to a malicious one and thereby the user can avoid installing the file in the device. This can help the user from falling into the trap of the running harmful files and hence protecting the data and information security. Antivirus software is quite expensive to operate and takes up a lot of space on the device. It consumes RAM and memory on a regular basis in order to keep the deity healthy. Whereas these machine-learning algorithms predict if an application is harmful or not based on its physical traits and behavior, the user must configure the information he knows about the specific program, and the trained model does the rest. The data set contains information such as app name, downloaded time, ram usage, behavior of the computer after download, permissions requested during installation, the presence or absence of a digital signature for the downloaded application, the source of the download, whether it is verified by several genuine applications or not, and finally whether the application is malicious or not. Numerous antivirus apps will gather this data using various post-installation detection methods, such as signature-based detection, behavior-based detection, heuristic-based detection, and sandbox detection.

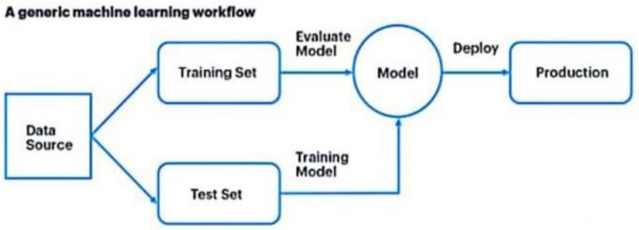
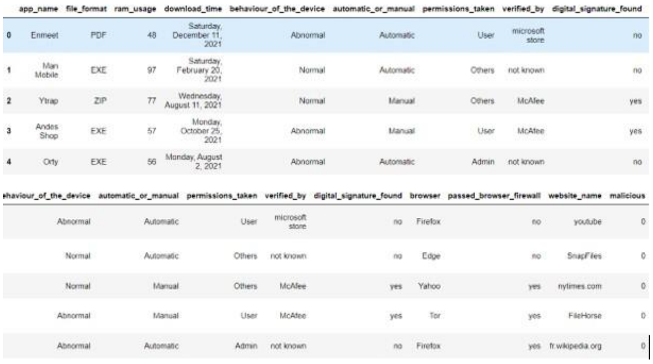


Figure 9: machine learning model process

A. Data set

The data set contains a wealth of information about the applications that is understandable to the average user. Machine-learning algorithms will differentiate between safe and malicious applications based on these attributes, and the features that assist us in the process include Application name, downloaded file type, RAM use, downloaded time, behavior of the device after download, automated or manual installation, permissions requested during installation confirmed by and sources, whether or not a digital signature was detected, the browser, passes or fails the browser firewall, website name, or source of the downloaded program, malicious or not being the target variable.



	app_name	file_format	ram_usage	download_time	behaviour_of_the_device	automatic_or_manual	permissions_taken	verified_by	digital_signature_found	browser	passed_browser_firewall	website_name	malicious
0	Enmeet	PDF	48	Saturday, December 11, 2021	Abnormal	Automatic	User	microsoft store	no	Firefox	no	youtube	0
1	Man Mobile	EXE	97	Saturday, February 20, 2021	Normal	Automatic	Others	not known	no	Edge	no	SnapFiles	0
2	Ytrap	ZIP	77	Wednesday, August 11, 2021	Normal	Manual	Others	McAfee	yes	Yahoo	yes	nytimes.com	0
3	Andes Shop	EXE	57	Monday, October 25, 2021	Abnormal	Manual	User	McAfee	yes	Tor	yes	FileHorse	0
4	Orty	EXE	56	Monday, August 2, 2021	Abnormal	Automatic	Admin	not known	no	Firefox	yes	fr.wikipedia.org	0

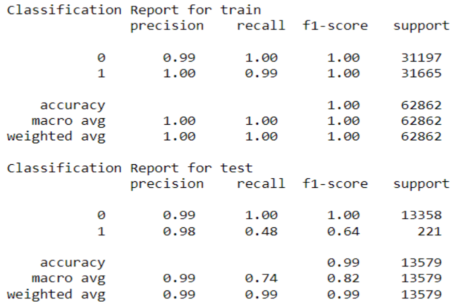
Figure 10:data set containing information about apps

B. Algorithms used

I implemented several machine algorithms in order to improve efficiency and accuracy like

- **Gradient boost**

The machine learning boosting system known as gradient boosting represents a decision tree for large and complex data. It is predicated on the idea that the next model will lower the overall prediction error when combined with the previous set of models. Decision trees are used to make the most accurate predictions. The gradient boosting method is also known as the statistical predictive algorithm. Even though it allows for the generalization and optimization of divergent loss functions, it still functions largely in the same way as earlier boosting methods. Processes for classification and regression frequently use gradient boosting.

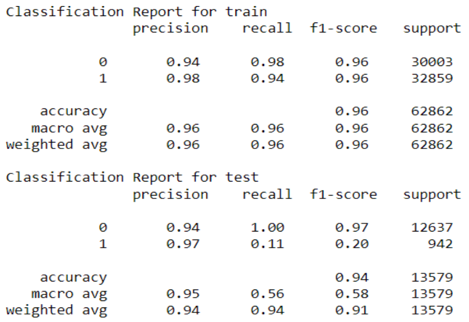


```
Classification Report for train
               precision    recall  f1-score   support

           0       0.99      1.00      1.00     31197
           1       1.00      0.99      1.00     31665

    accuracy                           1.00     62862
   macro avg       1.00      1.00      1.00     62862
weighted avg       1.00      1.00      1.00     62862

Classification Report for test
               precision    recall  f1-score   support

           0       0.99      1.00      1.00     13358
           1       0.98      0.48      0.64       221

    accuracy                           0.99     13579
   macro avg       0.99      0.74      0.82     13579
weighted avg       0.99      0.99      0.99     13579
```

Figure 10: results of random forest algorithm

- **Logistic regression**

Logistic regression is a well-known Machine Learning algorithm from the Supervised Learning method. It forecasts the categorical variables based on a set unconventional variable. A categorical dependent variable's output is predicted using logistic regression. As a result, the outcome must be categorical or discrete. It can be zero or one, true or False, and so on, but rather than presenting the actual values like 0 and 1, it presents the probability values that fall between zero and one.

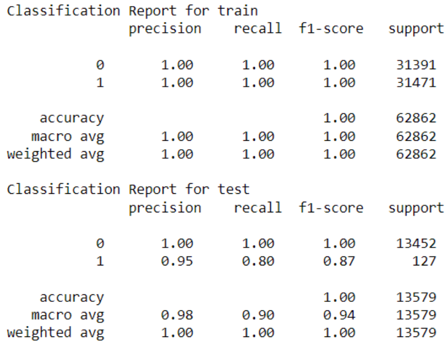


```
Classification Report for train
               precision    recall  f1-score   support

           0       0.94      0.98      0.96     30003
           1       0.98      0.94      0.96     32859

    accuracy                           0.96     62862
   macro avg       0.96      0.96      0.96     62862
weighted avg       0.96      0.96      0.96     62862

Classification Report for test
               precision    recall  f1-score   support

           0       0.94      1.00      0.97     12637
           1       0.97      0.11      0.20       942

    accuracy                           0.94     13579
   macro avg       0.95      0.56      0.58     13579
weighted avg       0.94      0.94      0.91     13579
```

Figure 11: results of logistic algorithm

- **Random Forest**

Random Forest is a popular supervised machine learning technique. It can be used in machine learning to solve classification and regression problems. It is based on the concept of ensemble learning, which is also the method of combining multiple classifiers to address a complex problem and improve the model's performance. Random Forest is a classifier that averages different decision trees on different subsets of a given dataset to improve the dataset's projected accuracy. Rather than relying solely on one decision tree, the random forest forecasts the correct outcome by taking into account the predictions made by each tree.

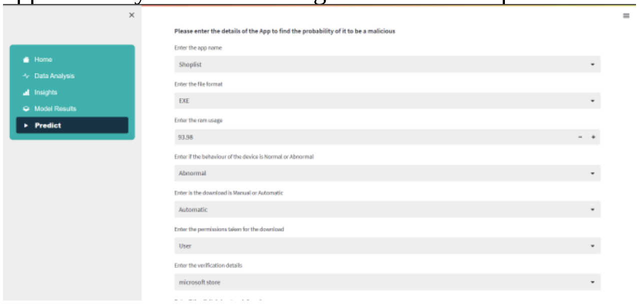


```
Classification Report for train
               precision    recall  f1-score   support

           0       1.00      1.00      1.00     31391
           1       1.00      1.00      1.00     31471

    accuracy                           1.00     62862
   macro avg       1.00      1.00      1.00     62862
weighted avg       1.00      1.00      1.00     62862

Classification Report for test
               precision    recall  f1-score   support

           0       1.00      1.00      1.00     13452
           1       0.95      0.80      0.87       127

    accuracy                           1.00     13579
   macro avg       0.98      0.90      0.94     13579
weighted avg       1.00      1.00      1.00     13579
```

Figure 12: results of random forest algorithm

C. User interface with Streamlit

Streamlit is a transparent Python framework that allows users to construct and share visually appealing, one-of-a-kind online apps for data processing and artificial intelligence. With the aid of this software, complex data apps may be designed and published.



Please enter the details of the App to find the probability of it to be a malicious

Enter the app name: Shoplist

Enter the file format: EXE

Enter the ram usage: 93.98

Enter if the behaviour of the device is Normal or Abnormal: Abnormal

Enter is the download is Manual or Automatic: Automatic

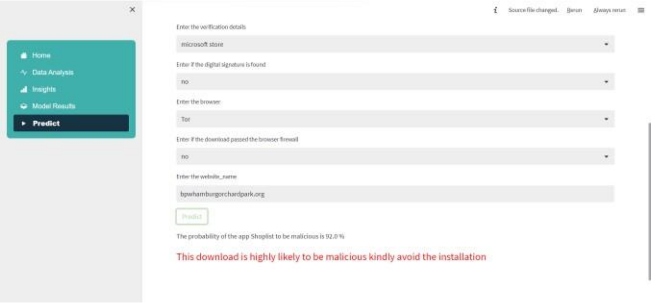
Enter the permissions taken for the download: User

Enter the verification details: microsoft store

Figure 13: user interface of running with machine learning model

IV. Results

Developed a machine learning models that predict the malicious applications with an accuracy of 0.99 percent. The random forest algorithm was chosen as the final model based on optimization and results. To determine how safe the downloaded application is, the user must provide specific information on a beautifully designed streamlit interface.



Enter the verification details

microsoft store

Enter if the digital signature is found

no

Enter the browser

Tor

Enter if the download passed the browser firewall

no

Enter the website_name

bpwhamburgorchardpark.org

The probability of the app Shoplist to be malicious is 92.0 %

This download is highly likely to be malicious kindly avoid the installation

Figure 14: final result of the proposed system

V. Conclusion

This paper described numerous hacking methods and their defenses from diverse angles. Hackers must be kept out of the network in order to secure sensitive data. existing system is expensive and time consuming compared to proposed system. Machine learning plays a key role in this project for predicting threat level of an application without even installing the application. I believe this paper helps readers enhance their understanding of cyber security and address security vulnerabilities in their computer operations. It also assists in the transmission of knowledge about emerging security concerns. Prevention is preferable to cure. Keep an eye out for cybercriminals.

VI. References

1. Yu, W., Yalin, Y., & Haodan, R. (2019, October). Research on the technology of trojan horse detection. In 2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA) (pp. 117-119). IEEE.
2. Al-Asli, M., & Ghaleb, T. A. (2019, April). Review of signature-based techniques in antivirus products. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.
3. Asish, M. S., & Aishwarya, R. (2019, March). Cyber security at a glance. In 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (Vol. 1, pp. 240-245). IEEE.
4. Rathore, H., Agarwal, S., Sahay, S. K., & Sewak, M. (2018, December). Malware detection using machine learning and deep learning. In International Conference on Big Data Analytics (pp. 402-411). Springer, Cham.
5. Namanya, A. P., Cullen, A., Awan, I. U., & Disso, J. P. (2018, August). The world of Malware: An overview. In 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 420-427). IEEE.
6. Bhardwaj, A., & Goundar, S. (2020). Keyloggers: silent cyber security weapons. Network Security, 2020(2), 14-19.
7. Parthy, P. P., & Rajendran, G. (2019, October). Identification and prevention of social engineering attacks on an enterprise. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-5). IEEE.
8. Kunwar, R. S., & Sharma, P. (2016, April). Social media: A new vector for cyber-attack. In 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring) (pp. 1-5). IEEE.
9. Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE Access, 8, 6249-6271.
10. Idika, N., & Mathur, A. P. (2007). A survey of malware detection Purdue University, 48(2), 32-46.