ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

Machine Learning Techniques for Polymorphic Malware Analysis and Identification

[1]Rajashekar Kandakatla
Research Scholar
Department of CSE
Bharath Institute of Higher Education and Research
Tamilnadu, India

[2]K. Rajakumari
Associate Professor
Department of CSE
Bharath Institute of Higher Education and Research
Tamilnadu, India

Abstract:- Internet users are now experiencing one of the biggest problem is malware. Polymorphic malware refers to harmful software and versatile compare to the other traditional viruses. Malware that is polymorphic continuously alters its signature characteristics to evade detection by conventional malware detection techniques that rely on signatures. In order to detect malware or harmful threats, we employed many machine learning approaches. Based on a high detection rate, best accuracy was selected by the algorithm in this method. One of the benefits by the confusion matrix is that to measure the number of false positives and also number of false negatives, providing deeper insights into the system's effectiveness. Specifically, it was demonstrated that the outcomes of analysis of malware and discovery using ML techniques to quantify the variation in correlation equilibrium integrals could enhance the security of computer networks by identifying malicious traffic on computer systems. According to the findings in percentage, support vector machine is 96.41, Convolutional neural networks is 98.76, Decision tree is 99 do better than the other classifiers to finding the accuracy. Malware detection capabilities of these algorithms were evaluated on a tiny False Positive Rate (Support Vector Machine is 4.63, Convolutional Neural Networks is 3.97 and Decision Tree is 2.01) in a particular dataset. Given the rise in sophistication and prevalence of malicious software, these findings are noteworthy.

Keywords:- *Machine Learning, Malicious Threats, Cyber Security, Cyber Attacks, Convolutional Neural Networks.*

I. INTRODUCTION

The most urgent issue in the field of contemporary technology at the moment is cyber attacks. The term suggests taking use of a system's weaknesses for malevolent ends, such stealing, altering, or destroying it. One type of cyber attack is malware. Cloud security protects data, applications, and infrastructure in cloud environments from cyber attacks and unlawful access. Cloud security includes encryption, access control, identity management, and network security protocols [1]. To prevent risks like data breaches, malware attacks, and insider threats, it's vital to implement strong security measures as cloud services become more widely used across sectors [2]. The program which is a set of instructions to developed to harm a any human, device, computer and organization is referred to as malware [3]. This extensive category encompasses threats such as viruses, Trojan-horses, ransom-ware, spy-ware, adware, rogue-software, wipers, scare-ware, and others. Without any knowing or any agreement from the users the

Program instructions are executed by the malicious software [4]. To find, if a particular software or network connection presents a safety threat, malware detection systems need to evaluate the data they have collected and learned from. For instance, to use a ML model for clearly explain the fundamental principles behind the patterns it has encountered [5, 6]. Take, for example, a machine learning system that is able to articulate directly the underlying principles of the patterns it has seen [7]. By leveraging feedback about how well they performed on prior jobs and using that information to make adjustments, machine learning-trained algorithms can become more predictive [8]. The suggested method is superior to alternatives, according to experiments [9]. Current ‘malware’ is in future more prevalent & complicated, effects a significant danger for the security of current ‘websites’ [10]. In Fig.1 displays many cyber attacks in the realm, often known as cyberspace. Malware is software or program developed specifically do harm to a network/system, such as observing users else theft the cash. ‘Malware’ assaults growing more widespread, In addition to the present threaten Internet of Things components, medicinal equipment, and environmental industrial monitoring systems. Latest spy-ware is disreputably difficult to discovery since that continuously modifies its program and behavior. The rise of mal-ware is made ineffective based on the old signature defenses. Therefore, a broader range of protective strategies is necessary [11].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

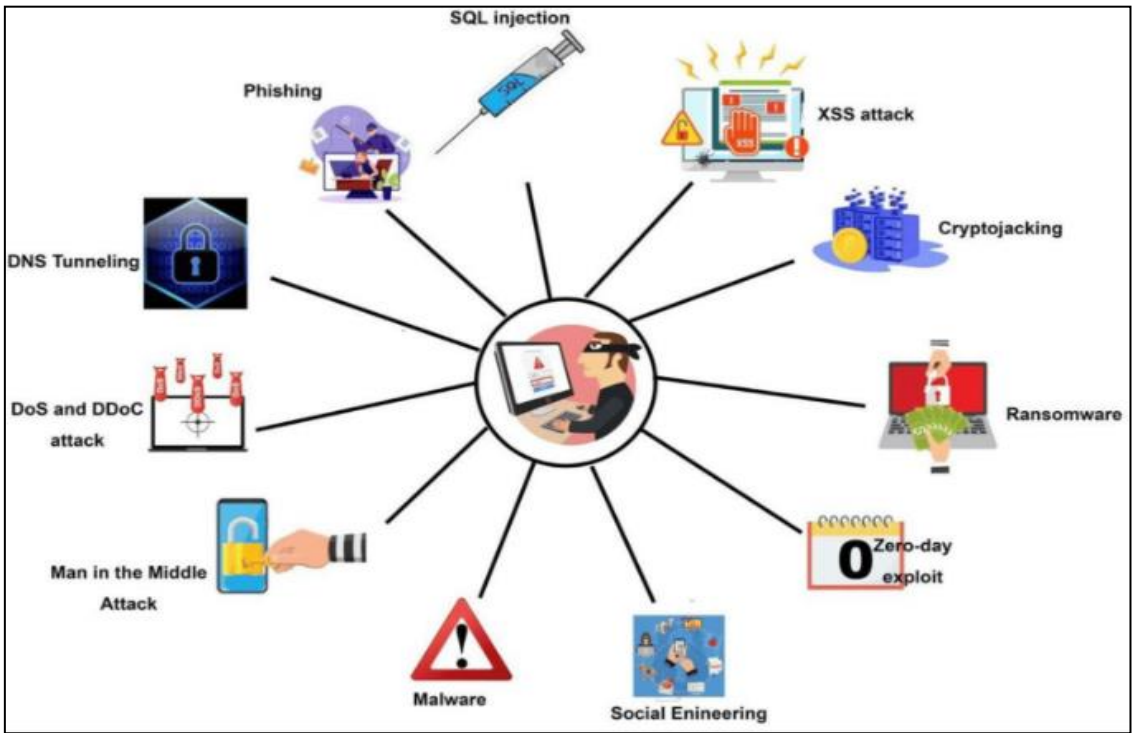

Fig 1 Types of Cyber Attacks

The static learning methods and dynamic learning methods can be employed to recognize the behavioral patterns among mal-ware from the same family [12]. Fixed analysis examines the contents of malicious files without running them, while dynamic analysis observes their behavior by tracking data flows, recording function calls, and incorporating monitoring code into dynamic binaries [13]. ML methods can influence both fixed and behavioral data for understand constantly developing nature of modern mal-ware, enabling to detect more sophisticated attacks that signature-based methods [14]. Figure 2 illustrates Martin's (2018) Cyber Kill Chain, which serves as a framework for defending against cyber attacks and implementing network security strategies. In February 2020, AWS experienced a significant Distributed Denial-of-Service (DDoS) attack [15]. A company endured a Distributed Denial-of-Service attack that peaked at 2.3 Tbps, achieving a packet forwarding rate of 293.1 million packets per second (Mpps) and a request rate of 694,201. This incident is considered one of the largest DDoS attacks on record. In July 2020, three hackers infiltrated Twitter, gaining control of several high-profile accounts [16]. National Health Serviced data from England indicates that the Wanna-Cry ransom-ware attack in 2017 impacted over 300,000 systems across 150 nations, resulting in billions of pounds in recovery costs [17].

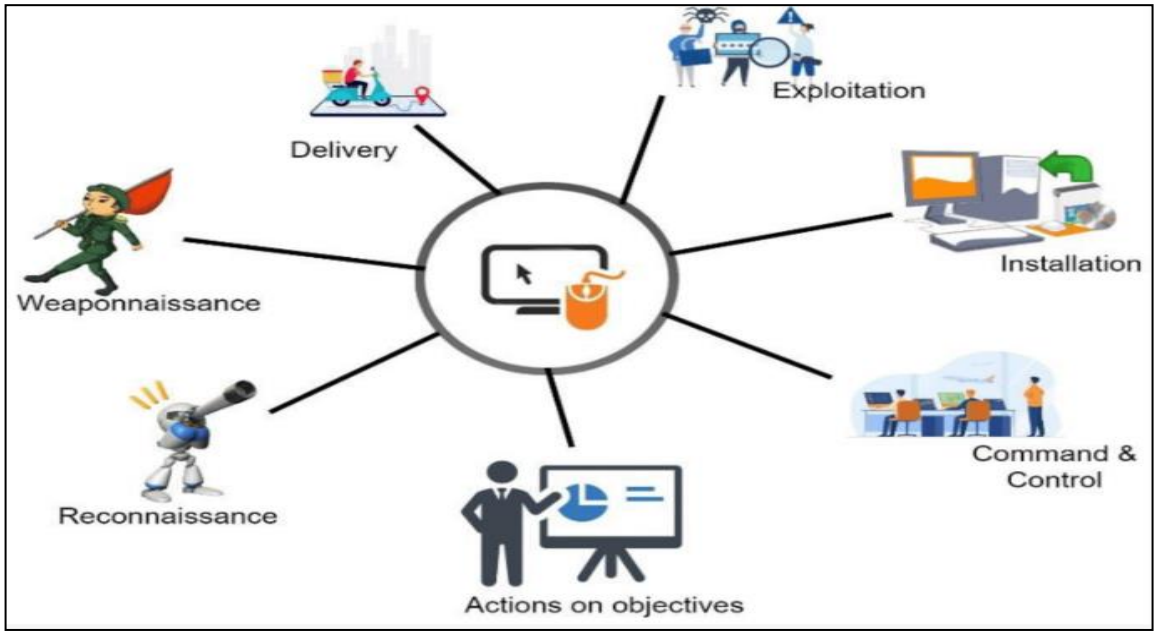

Fig 2 Martin Cyber Kill Chain for Preventing Cyber Incursion Activities

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

In 2017, as part of its ongoing strategy to undermine neighboring countries, Russia launched a cyber attack on Ukraine's energy infrastructure [18]. This incident marked the first instance of Russia showcasing its ability to conduct large-scale cyber warfare. Although it occurred a year after Russia's invasion of Crimea, which is generally viewed as the beginning of the conflict with Ukraine, this complex operation represented the first successful breach of a power facility [19]. The Russian cyber military unit known as Sandworm targeted the command center, exploiting a vulnerability that allowed them to seize control of the substation's computer systems, leading to its failure. Soon after, additional substations were attacked. The incident is estimated to have resulted in between 200,000 and 300,000 injuries [20].

II. LITERATURE REVIEW

This work examined in many strategies for ma-lware classification and discovery, focusing on how researchers have created methods to identify harmful intent in data by using both ML and DL [21]. “Armaan in 2021 showcased and assessed the precision of various models. Without data, no application designed for a digital environment can function effectively” [22]. Numerous cyber threats exist, making it essential to implement measures to safeguard data. While feature selection poses challenges in model development, ML stands out as an advanced approach that allows for accurate predictions. Table.1 shows the file types of data sets [23]. IT security professionals can utilize malware analysis tools to detect trends. The rise of tools that examine malware samples and assess their level of threat significantly aids the cybersecurity field. These tools help monitor security alerts and thwart malware attacks. If malware is deemed harmful, it must be eliminated before it can spread further. The popularity of malware analysis is increasing as it helps organizations lessen the impact of the growing number of malware threats and the evolving sophistication of malware targeting [24].

Table 1 File Types of Data Sets

Type of file	No. of files
Clean-ware	2711
Trojan	2563
Back-door	3654
Work	921
Root-kit	2834
Exploit	652
Virus	921
Others	3138
Total	17394

In 2018, Chowdhury was proposed an efficient mal-ware discovery approach that utilizes ML classification techniques. We explored whether modifying certain factors could enhance the accuracy of malware classification [25]. Our approach included support for N-grams and API calls. The effectiveness and reliability of our proposed method were validated through experimental evaluation. Future studies will aim to integrate a broader range of features to enhance detection accuracy while minimizing false positives. The performance results for competing methods are presented in Table 2, clearly indicating that our Chowdhury [25] strategy outperformed the others.

Table 2 Comparisons of Classifier Results

Methods	FPR	TPR	Accuracy
CNN	3.97	99.22	98.76
KNN	3.42	96.17	95.02
Random Forest	6.5	95.9	92.01
Naïve Byes	13	90	89.71
SVM	4.63	98	96.41
DT	2.01	99.07	99

The stability of the world is currently under grave jeopardy due to the proliferation of malicious software. Malware spread around the world in the 1990s as the no.of networked computers rose along with the prevalence of malicious software. To address this issue, a number of preventative strategies have been created. Regretfully, traditional defenses are unable to keep up with the most recent threats that malware developers have created to circumvent protection software. Scholars have shifted their focus from malware detection research to machine learning algorithm strategies in recent years. In this work, we present a security mechanism that evaluates three malware detection techniques using machine learning algorithms and chooses the most effective one. Statistics on a small dataset indicate that the decision tree approach has the highest detection rate and the lowest false positive rate is 0.021% and the highest detection accuracy is 99.01%. It repeats to implement and proliferate at an alarming rate. In order to evaluate and measure the detection performance of the classifier that extracted features from PE data using static analysis, Nur (2019) looked at three ML classifiers. Together, we trained machine learning algorithms to differentiate between

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

dangerous and non-damaging content [26]. The DT machine learning method was the most successful classifier we examined, with 99% accuracy, as shown in Table 2. The rapid proliferation of malware on the Internet has given its creators access to a wide range of tools [27]. The main benefit for the users may check legitimacy of a file before opening it, which lowers the chance of unintentionally installing harmful software [28].

III. RESEARCH PROBLEM

The potentially harmful element of malware is found using fixed or behavioral analysis. Fixed analysis used to break down a virus, focuses on parsing ma-lware binaries to identify dangerous strings [29]. Behavioral analysis includes observing the harmful software while its works in a monitored closed environment, such a online system computer. When examining malware, it is advised to use both methods even though each has advantages and disadvantages [30]. It's possible that if there were less detrimental traits, malware detection accuracy may rise. The researcher would then have more time to review the data that was collected. We are concerned that too many features are being used to detect malware when a few more powerful features would work just as well. Selecting which detrimental traits to employ begins with identifying possible methods or algorithms. We need solutions that could drastically reduce the attributes now needed to identify malware and identify malware that has never been detected before [31].

IV. METHODOLOGY

This research article introduces the components and procedures of a typical machine learning process for malware detection and classification. With an emphasis on deep learning methods, it also assesses the most recent developments and trends in the field and looks at the challenges and limitations of this type of workflow. A description of the research study's recommended methodology is provided below [32]. Figures 3 and 4 illustrate the architecture and ML malware detection technique.

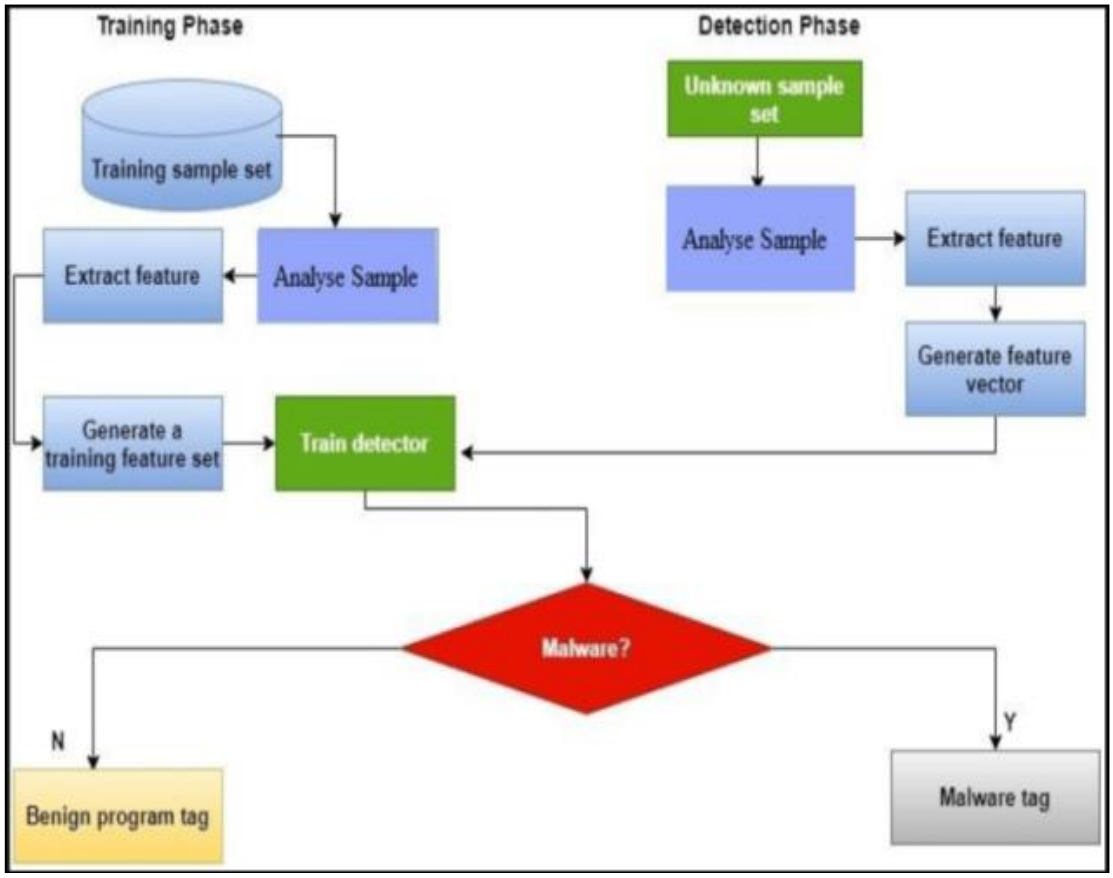

Fig 3 Architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

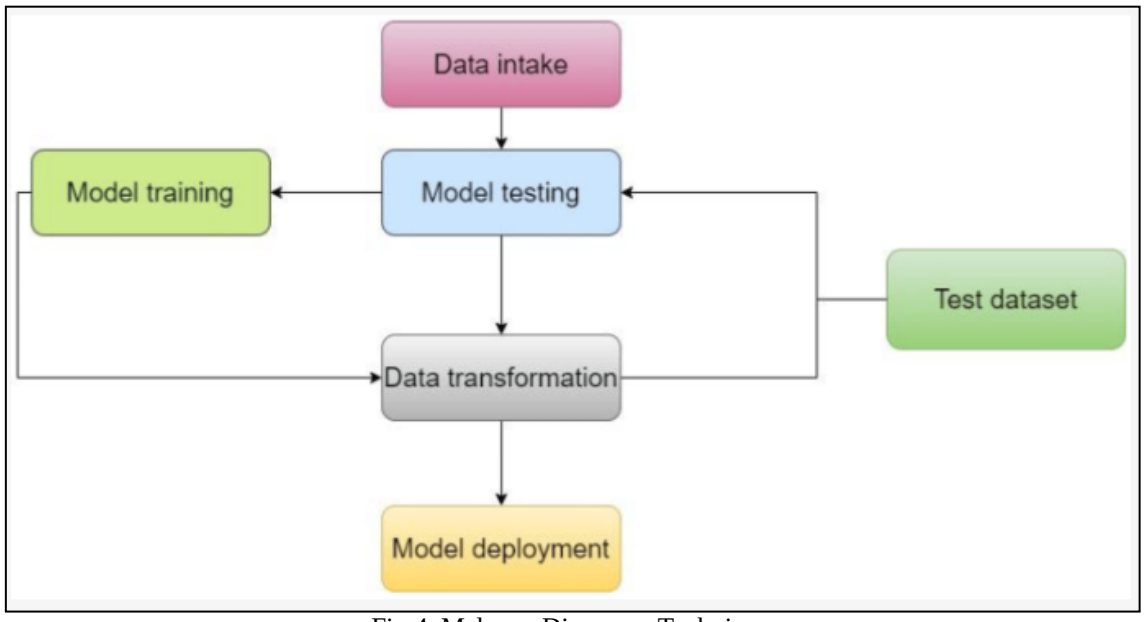

Fig.4. Malware Discovery Technique

➢ *Data Set:*

All of the data utilized in this study was provided by the Canadian Institute for Cybersecurity. Several data files, including log data from different types of malware, are included in the collection [33]. A variety of models can be trained using the recovered log features. There were about 51 distinct malware families in the samples. Over 17,394 data points from multiple sources were included in the dataset, which was arranged into 17,394 rows and 279 columns.

➢ *Pre-Processing:*

The files in the file system were unprocessed executables that held data in binary code. We got them ready before we started our investigation. A secure environment, commonly referred to as a virtual machine (VM), was required in order to unpack the executables. PEiD software allows compressed executables to be automatically unpacked [34].

➢ *Data Set:*

Tens of thousands of attributes are frequently seen in twentieth-century datasets. As feature counts rose in recent years, it became clear that the machine learning model that was produced was over fit [35]. We addressed this problem by generating a smaller set of features from a larger set; this method is frequently used to use fewer features while maintaining the same degree of precision. By keeping the most valuable features and eliminating those that weren't beneficial for data analysis, this study aimed to enhance the current collection of dynamic and static characteristics [36].

➢ *Features Selection:*

After complete feature extraction, which included the identification of further characteristics, feature selection was carried out. Because feature selection involved choosing features from a pool of recently identified qualities, it was a crucial step in increasing accuracy, streamlining the model, and reducing over fitting. To find dangerous code in software, researchers used a range of feature classification approaches in the past. This work made extensive use of the feature rank approach, which is especially effective in choosing the pertinent features for creating malware detection models [37, 38].

V. RESULTS AND DISCUSSION

The two primary stages of the classification procedure were training and testing. A system was trained using both safe and dangerous files [39]. A learning algorithm was used to train an automatic classifier. With every piece of data it examined, the classifiers got better. A classifier was given a collection of new files throughout the testing phase, some of which were harmful and some of which weren't. The Classifier determined whether the files were malicious or cleans [40]. According to Figure 5, Accuracy of False Positive Rate is 2.01%, whereas Decision Tree is 99% and True Positive Rate is 99.07%. DT performed better than all other ML methods, as the confusion matrix makes evident [41].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

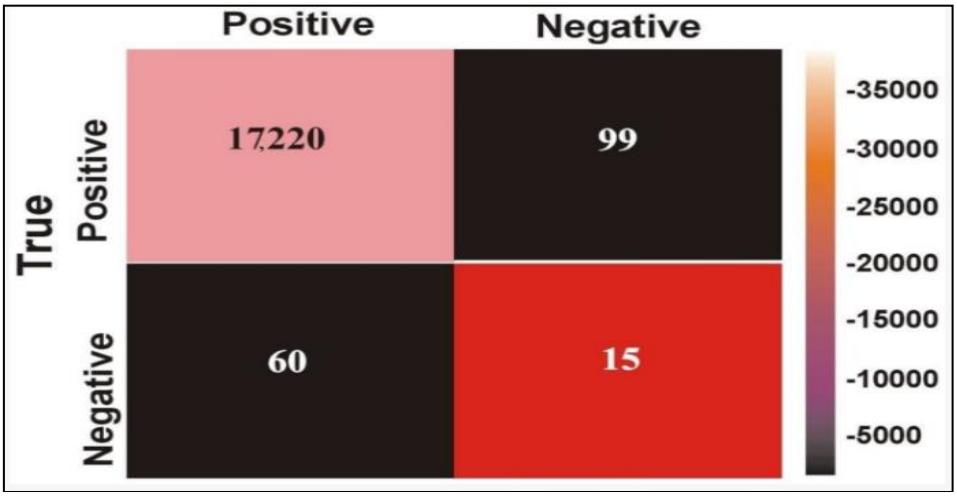

Fig 5 Accuracy Percentages of Algorithms

We experimentally tested our proposed malware categorization and detection method on a collection of malware and clean ware [42]. Using classifiers, we assessed and detected malware. With accuracy scores of 95.02% for KNN, 98.76% for CNN, 89.71% for Naïve Byes, 92.01% is RF, 96.41% for Support Vector Machine, and 99% is Decision Tree, we determined that Decision Tree is the best method for identification of malware based on statistical analysis of Table 2. CNN is 2nd best method for malware discovery, while Support Vector Machine is 3rd finest model, according to the True Positive Rates in percentage of the classifiers of K-nearest neighbors is 96.17, Convolutional Neural Networks is 99.22, Naïve Byes = 90, RF is 95.9, Support Vector Machine is 98, and Decision Tree is 99.07. The FPRs (%) for a number of classifiers are shown in Table 2, including DT (2.01%), Random Forest (6.5%), SVM (4.63%), CNN (3.97%), Naïve Byes (13%), and KNN (3.42%). For all practical reasons, we assumed that these classifiers performed similarly well and had high accuracy. It is clear that the highest TPR (%) rate and accuracy are obtained when using these optimal algorithm methods for Decision Tree is 99, Support Vector Machine is 96.41, and Convolutional Neural Networks is 98.76 to detect malware, suggesting that DT is the best option to discovery of mal-ware.

VI. CONCLUSION

This study proves that ML methods give solutions to discovery of mal-ware have recently drawn more attention from academics. To detect malware, we offered a defense methods calculate the three ML algorithm methods and select the best effective one. The outcome proves that in terms of detection accuracy, Decision Tree is 99% is best compare to other classifiers. And when consider the particular dataset, the effectiveness of the methods in detecting malware for False Positive Rate is high for Support Vector Machine is 4.63%. In order to ascertain and measure the accuracy identification a machine learning classifier that used fixed analysis to finding the features from PE data, we contrasted it with other classifiers in this experiment. This work has enabled ML Methods to discriminate between benign and harmful data. After assessment of all the classifiers, the Decision Tree ML method had finest accuracy i.e. 99%. Fixed analysis based on PE information and carefully chosen data has showed promise in experimental results, possibly providing the discovery accuracy and accurately describing mal-ware. One major benefit is that we don't need to do any tests to determine whether the data is malicious. A dataset obtained from the CIS was used to train, test, and assess the efficacy of the three machine learning models (DT, CNN, and SVM).

REFERENCES

[1]. T. Bhaskar, M.N. Narsaiah and M. Ravikanth, “Central Medical Centre Healthcare Data Security with Lightweight Blockchain Model in IoT Sensor Environment,” Journal of Sensors, IoT & Health Sciences, vol.01, no.01, pp.15-26,2023.

[2]. M. Bakro, R.R. Kumar, M. Husain, Z.Ashraf, A. Ali et al., “Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model,” IEEE Access, 2024.

[3]. Nikam, U.V.; Deshmuh, V.M. Performance evaluation of machine learning classifiers in malware detection. In Proceedings of the 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 23–24 April 2022; pp. 1–5.

[4]. Akhtar, M.S.; Feng, T. IOTA based anomaly detection machine learning in mobile sensing. *EAI Endorsed Trans. Create. Tech.* 2022, *9*, 172814.

[5]. Sethi, K.; Kumar, R.; Sethi, L.; Bera, P.; Patra, P.K. A novel machine learning based malware detection and classification framework. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019; pp. 1–13.

[6]. Abdulbasit, A.; Darem, F.A.G.; Al-Hashmi, A.A.; Abawajy, J.H.; Alanazi, S.M.; Al-Rezami, A.Y. An adaptive behavioral-based increamental batch learning malware variants detection model using concept drift detection and sequential deep learning. *IEEE Access* 2021, *9*, 97180–97196.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

[7]. Feng, T.; Akhtar, M.S.; Zhang, J. The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Trans. Create. Tech.* 2021, *8*, 170285.
[8]. Sharma, S.; Krishna, C.R.; Sahay, S.K. Detection of advanced malware by machine learning techniques. In Proceedings of the SoCTA 2017, Jhansi, India, 22–24 December 2017.
[9]. Chandrakala, D.; Sait, A.; Kiruthika, J.; Nivetha, R. Detection and classification of malware. In Proceedings of the 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 8–9 October 2021; pp. 1–3.
[10]. Zhao, K.; Zhang, D.; Su, X.; Li, W. Fest: A feature extraction and selection tool for android malware detection. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 714–720.
[11]. Akhtar, M.S.; Feng, T. Detection of sleep paralysis by using IoT based device and its relationship between sleep paralysis and sleep quality. *EAI Endorsed Trans. Internet Things* 2022, *8*, e4.
[12]. Gibert, D.; Mateu, C.; Planes, J.; Vicens, R. Using convolutional neural networks for classification of malware represented as images. *J. Comput. Virol. Hacking Tech.* 2019, *15*, 15–28.
[13]. Firdaus, A.; Anuar, N.B.; Karim, A.; Faizal, M.; Razak, A. Discovering optimal features using static analysis and a genetic search based method for Android malware detection. *Front. Inf. Technol. Electron. Eng.* 2018, *19*, 712–736.
[14]. Dahl, G.E.; Stokes, J.W.; Deng, L.; Yu, D.; Research, M. Large-scale Malware Classification Using Random Projections And Neural Networks. In Proceedings of the International Conference on Acoustics, Speech and Signal Processing-1988, Vancouver, BC, Canada, 26–31 May 2013; pp. 3422–3426.
[15]. Akhtar, M.S.; Feng, T. An overview of the applications of artificial intelligence in cybersecurity. *EAI Endorsed Trans. Create. Tech.* 2021, *8*, e4.
[16]. Akhtar, M.S.; Feng, T. A systemic security and privacy review: Attacks and prevention mechanisms over IOT layers. *EAI Endorsed Trans. Secur. Saf.* 2022, *8*, e5.
[17]. Anderson, B.; Storlie, C.; Lane, T. "Improving Malware Classification: Bridging the Static/Dynamic Gap. In Proceedings of the 5th ACM Workshop on Security and Artificial Intelligence (AISec), Raleigh, NC, USA, 19 October 2012; pp. 3–14.
[18]. Varma, P.R.K.; Raj, K.P.; Raju, K.V.S. Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 294–299.
[19]. Akhtar, M.S.; Feng, T. Comparison of classification model for the detection of cyber-attack using ensemble learning models. *EAI Endorsed Trans. Scalable Inf. Syst.* 2022, *9*, 17329.
[20]. Rosmansyah, W.Y.; Dabarsyah, B. Malware detection on Android smartphones using API class and machine learning. In Proceedings of the 2015 International Conference on Electrical Engineering and Informatics (ICEEI), Denpasar, Indonesia, 10–11 August 2015; pp. 294–297.
[21]. Tahtaci, B.; Canbay, B. Android Malware Detection Using Machine Learning. In Proceedings of the 2020 Innovations in Intelligent Systems and Applications Conference (ASYU), Istanbul, Turkey, 15–17 October 2020; pp. 1–6.
[22]. Baset, M. Machine Learning for Malware Detection. Master's Dissertation, Heriot Watt University, Edinburg, Scotland, December 2016.
[23]. Akhtar, M.S.; Feng, T. Deep learning-based framework for the detection of cyberattack using feature engineering. *Secur. Commun. Netw.* 2021, *2021*, 6129210.
[24]. Altaher, A. Classification of android malware applications using feature selection and classification algorithms. *VAWKUM Trans. Comput. Sci.* 2016, *10*, 1.
[25]. Chowdhury, M.; Rahman, A.; Islam, R. *Malware Analysis and Detection Using Data Mining and Machine Learning Classification*; AISC: Chicago, IL, USA, 2017; pp. 266–274.
[26]. Patil, R.; Deng, W. Malware Analysis using Machine Learning and Deep Learning techniques. In Proceedings of the 2020 SoutheastCon, Raleigh, NC, USA, 28–29 March 2020; pp. 1–7.
[27]. Gavriluţ, D.; Cimpoesu, M.; Anton, D.; Ciortuz, L. Malware detection using machine learning. In Proceedings of the 2009 International Multiconference on Computer Science and Information Technology, Mragowo, Poland, 12–14 October 2009; pp. 735–741.
[28]. Pavithra, J.; Josephin, F.J.S. Analyzing various machine learning algorithms for the classification of malwares. *IOP Conf. Ser. Mater. Sci. Eng.* 2020, *993*, 012099.
[29]. Vanjire, S.; Lakshmi, M. Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning. In Proceedings of the 2021 International Conference on Artificial Intelligence and Machine Vision (AIMV), Gandhinagar, India, 24–26 September 2021; pp. 1–4.
[30]. Agarkar, S.; Ghosh, S. Malware detection & classification using machine learning. In Proceedings of the 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), Gunupur Odisha, India, 16–17 December 2020; pp. 1–6.
[31]. Sethi, K.; Chaudhary, S.K.; Tripathy, B.K.; Bera, P. A novel malware analysis for malware detection and classification using machine learning algorithms. In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 13–15 October 2017; pp. 107–113.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24NOV1395

[32]. Ahmadi, M.; Ulyanov, D.; Semenov, S.; Trofimov, M.; Giacinto, G. Novel feature ex-traction, selection and fusion for effective malware family classification. In Proceedings of the sixth ACM conference on data and application security and privacy, New Orleans, LA, USA, 9–11 March 2016; pp. 183–194.
[33]. Damshenas, M.; Dehghantanha, A.; Mahmoud, R. A survey on malware propagation, analysis and detec-tion. *Int. J. Cyber-Secur. Digit. Forensics* 2013, *2*, 10–29.
[34]. Saad, S.; Briguglio, W.; Elmiligi, H. The curious case of machine learning in malware detection. *arXiv* 2019, arXiv:1905.07573.
[35]. Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. *Indones. J. Electr. Eng. Comput. Sci.* 2019, *16*, 435.
[36]. Firdausi, I.; Lim, C.; Erwin, A.; Nugroho, A. Analysis of machine learning techniques used in behavior-based malware detection. In Proceedings of the 2010 Second International Conference on Advances in Computing, Control, and Telecommunication Technologies, Jakarta, Indonesia, 2–3 December 2010; pp. 201–203.
[37]. Hamid, F. Enhancing malware detection with static analysis using machine learning. *Int. J. Res. Appl. Sci. Eng. Technol.* 2019, *7*, 38–42.
[38]. Prabhat, K.; Gupta, G.P.; Tripathi, R. TP2SF: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* 2021, *115*, 101954.
[39]. Kumar, P.; Gupta, G.P.; Tripathi, R. A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks. *J. Ambient Intell. Human. Comput.* 2021, *12*, 9555–9572.
[40]. Prabhat, K.; Gupta, G.P.; Tripathi, R. Design of anomaly-based intrusion detection system using fog computing for IoT network. *Aut. Control Comp. Sci.* 2021, *55*, 137–147.
[41]. Prabhat, K.; Tripathi, R.; Gupta, G.P. P2IDF: A Privacy-preserving based intrusion detection framework for software defined Internet of Things-Fog (SDIoT-Fog). In Proceedings of the Adjunct Proceedings of the 2021 International Conference on Distributed Computing and Networking (ICDCN ‘21), Nara, Japan, 5–8 January 2021; pp. 37–42.
[42]. Kumar, P.; Gupta, G.P.; Tripathi, R. PEFL: Deep privacy-encoding-based federated learning framework for smart agriculture. *IEEE Micro* 2022, *42*, 33–40.