

Malware Detection using CNN+LSTM

Detecting malware in PE files

Agaaz Singhal, Ayush Sharma,
Shikhar Beriwal

MLPR Presentation

Ransomware Attack Targets VMware ESXi Servers Worldwide



Financial Services Firm NCR Hit by Ransomware Attack, Disrupting Aloha and Back Office Products

 SCOTT IKEDA · APRIL 25, 2023

Titans in crisis: unraveling the MGM and Caesars ransomware timeline

Updated on: November 15, 2023 12:53 PM 

Dallas Ransomware Attack Affects 30,253 People

Author : Sangfor Technologies Published Date : 29 Aug 2023 Last Modified Date : 31 Aug 2023

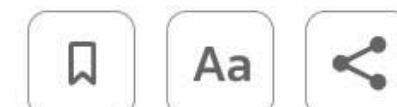
Ransom paid for NoEscape attack on Hawai'i Community College

SC Staff · July 31, 2023

Royal Mail faces threat from ransomware group LockBit

Reuters

February 8, 2023 5:33 AM GMT+5:30 · Updated a year ago



Problem



How are major malware attacks executed?


- Kaspersky Lab detected around 360,000 malware instances daily in 2020.
- Malicious programs infiltrate systems through various methods: script-based, document-based, exploits, memory injection, etc.
- Over 90% of daily detections involve malware utilizing Windows PE Files, emphasizing their dominance as a primary vehicle for malware propagation.


Why are current methods of malware detection failing?

- Traditional detection relies on matching malware signatures against a known threat database, but it's limited to known threats.
- ML-based techniques like SVM and Random Forest require sample collection and complex feature engineering, which demands human expertise.
- Challenges like adversarial ML emphasize the necessity for robust and adaptive approaches in malware detection.

Literature Review

Robust Detection Model for Portable Execution Malware

 The research paper "Robust Detection Model for Portable Execution Malware" explores malware detection in PE files using PCA and LDA for dimension reduction, along with a novel adversarial attack method, evaluated using the FFRI Dataset 2018.


 Limitations include the model's heavy reliance on dimension reduction, affecting performance and adaptability, and its residual vulnerability to novel adversarial attacks, highlighting ongoing challenges in robustness.


Malware Prediction Classifier using Random Forest Algorithm

The paper aims to improve unknown malware detection using the Random Forest algorithm for dynamic analysis, overcoming the time and resource constraints of traditional static tools. It demonstrates that the Random Forest has lower log loss errors compared to KNN, logistic regression, decision trees, and ADA boost.

The model exhibited overfitting issues due to poor generalization of the Random Forest Classifier (RFC).

Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time

 The research paper details using CNNs to detect fileless malware by converting network traffic into images. Though it focuses on network traffic rather than PE files

 Limitations include reliance on image conversion for feature extraction, which may not capture all data nuances, and the model's specific effectiveness against fileless malware, requiring adaptations for broader malware detection in PE files

Literature Review In Depth

Robust Detection Model for Portable Execution Malware

Robust Detection Model for Portable Execution Malware

1st Wanjia Zheng
University of Tsukuba
Tsukuba, Japan
s1830141@s.tsukuba.ac.jp

2nd Kazumasa Omote
University of Tsukuba
Tsukuba, Japan
omote@risk.tsukuba.ac.jp

Abstract—With recent technological developments, it has become natural for personal computers and Internet of Things(IoT) devices, such as smartphones and tablets, to remain constantly connected to the Internet. Malicious attackers are known to abuse malware to achieve their nefarious purposes, necessitating the implementation of defense systems as protection. Methods such as machine learning-based techniques, which have been utilized with great success in various fields such as image recognition and processing, and voice recognition, are used to prevent cyberattacks caused by malware. However, several adversarial attack methods have been proposed in recent years to induce malfunctions in machine learning-based models. In this study, we focus on malware detection field and treat the aforementioned issue from the perspectives of both attackers and defenders; subsequently, we propose a novel adversarial attack method, named IMAGE_RESOURCE attack, and a robust malware detection model, respectively, using dimension reduction and machine learning techniques. The robustness of the proposed model is evaluated using portable execution (PE) surface information obtained from

In recent years, several adversarial attack methods have been proposed to induce malfunctions in machine learning-based models [7], [10], [11], [15], [19], [20]. Current malware detection tool utilized by companies that aim to avoid false positives, was also used to successfully generate adversarial examples [2]. Thus, in this study, we focus on potential risks in machine learning-based malware detection systems and address this issue from the perspective of both attackers and defenders—we propose a novel adversarial attack named IMAGE_RESOURCE attack and a robust malware detection model, respectively, using dimension reduction and machine learning technology. Portable execution (PE) surface information obtained from the FFRI Dataset 2018 [18] is used to evaluate the proposed attack method and detection model. During robustness evaluation, distances (e.g., Euclidean distance) between the malware and benign files are measured.

Machine Learning Model Techniques Used:

- **Dimension Reduction (PCA and LDA):** Uses PCA and LDA to reduce data dimensionality, enhancing model performance.
- **Adversarial Attack Method (IMAGE_RESOURCE attack):** Introduces a novel technique that manipulates IMAGE_RESOURCE data in PE files.

Limitations of the Proposed Techniques:

- **Dependence on Dimension Reduction:** Effectiveness heavily relies on dimension reduction, potentially losing critical information.
- **Specificity to PE Files:** Tailored specifically to PE files, limiting broader applicability.
- **Adversarial Attack Vulnerability:** Remains susceptible to novel adversarial attacks, showing ongoing robustness challenges.

Literature Review In Depth

Malware Prediction Classifier using Random Forest Algorithm

Malware Prediction Classifier using Random Forest Algorithm

Hasmitha Dasari¹, Balarka Pradhyumna Danduboina², Dr. M. Chinna Rao³

^{1,2}Department of Computer Science and Engineering, Lingayas Institute of Management and Technology
Vijayawada, Andhra Pradesh, India

³Professor, Department of Computer Science and Engineering, Lingayas Institute of Management and
Technology, Vijayawada, Andhra Pradesh, India

Abstract— Windows devices are also becoming more popular and are more defenseless to malware attacks. Malware is computer code that is designed to harm the operating system and has various names, including adware, spyware, viruses, worms, trojans, backdoors, ransomware and command and control (C&C) bots, depending on its function. Malware attacks on systems are increasing as a result of increased internet use. The detection of unknown malware has been attempted using several strategies, but none of them have been successful. To deal with these threats, proposed research utilized dynamic malware research based on machine learning. Many malicious software-scanning

consider when it comes to computer security. The Malware Detection System is employed in many kinds of situations. Although several techniques have been developed to detect malware in its early stages of development, they have yet to detect malware cases. In the proposed work, a novel dynamic malware method is used since it has multiple execution paths and can cause destructive behavior. Malware analysis is a method for studying malicious activities and determining how to analyze malware's components and behavior. In this paper, the dynamic

Techniques Used

- 1. Dynamic Malware Analysis:** The study emphasizes dynamic analysis over static, allowing malware to run in a controlled environment to observe its behavior.
- 2. Random Forest Algorithm:** Utilized for its effectiveness in classifying malware based on behavior patterns identified during dynamic analysis.

Limitations

- **Overfitting:** The paper mentions the challenge of model overfitting, which can lead to poor generalization on unseen data. This is a common issue with complex models like Random Forest when trained on limited data.
- **Data Dependency:** The effectiveness of the model heavily relies on the quality and representativeness of the training data. Incomplete or biased data could lead to less effective malware detection.

Literature Review In Depth

Machine learning based fileless malware traffic classification using image visualization

Machine learning based fileless malware traffic classification using image visualization

Fikirte Ayalke Demmese^{1*}, Ajaya Neupane², Sajad Khorsandroo¹, May Wang², Kaushik Roy¹ and Yu Fu²

Abstract

In today's interconnected world, network traffic is replete with adversarial attacks. As technology evolves, these attacks are also becoming increasingly sophisticated, making them even harder to detect. Fortunately, artificial intelligence (AI) and, specifically machine learning (ML), have shown great success in fast and accurate detection, classification, and even analysis of such threats. Accordingly, there is a growing body of literature addressing how subfields of AI/ML (e.g., natural language processing (NLP)) are getting leveraged to accurately detect evasive malicious patterns in network traffic. In this paper, we delve into the current advancements in ML-based network traffic classification using image visualization. Through a rigorous experimental methodology, we first explore the process of network traffic to image conversion. Subsequently, we investigate how machine learning techniques can effectively leverage image visualization to accurately classify evasive malicious traces within network traffic. Through the utilization of production-level tools and utilities in realistic experiments, our proposed solution achieves an impressive accuracy rate of 99.48% in detecting fileless malware, which is widely regarded as one of the most elusive classes of malicious software.

Keywords Network security, Traffic classification, Fileless malware, Image visualization, Machine learning, Intrusion detection

Introduction

Network traffic flow classification is an essential network function that paves the way for dynamic and agile network management. It empowers network operators to handle different service requirements and constraints

traffic which ranges from malware infection to distributed denial of service (DDoS) attacks. Hence, it is essential to identify malicious network traffic that targets the underlying devices.

Fileless malware (Kumar 2020) is a type of evasive mal-

Machine Learning Model Techniques Used:

- **Convolutional Neural Networks (CNNs):** Employed for classifying network traffic that has been converted into images to detect fileless malware.

Limitations of the Proposed Techniques:

- **Dependence on Image Conversion:** The model's performance is heavily reliant on the effective transformation of network traffic into images, which may not always capture essential malicious behaviors.
- **Specificity to Network Traffic:** While effective in classifying network traffic, the technique might require significant adjustments or may not be directly applicable for analyzing Portable Executable (PE) files, which are central to your project.
- **Complexity in Visual Analysis:** The method assumes that visual patterns associated with malware can be consistently and accurately captured in images, which may not hold true across different malware types or attack vectors.

Datasets

Training Dataset + Benchmark Comparison

RAW PE AS IMAGE

- **Features:** Static analysis data represented as a 32 x 32 greyscale image flattened to a 1024-byte vector.
- **About:** The dataset includes static analysis data converted into 32x32 greyscale images and 1024-byte vectors.
- **EgSource:** virusshare.com, and goodware samples are from portableapps.com and Windows 7 x86 directories.

<https://www.kaggle.com/datasets/ang3loliveira/malware-analysis-datasets-raw-pe-as-image/data>

Benchmark Dataset

MALVIS DATASET

- **Features:** Comprises RGB images in two resolutions (224x224 and 300x300) for deep learning.
- **About:** Contains 26 classes, including one "legitimate" class, for malware recognition studies.
- **Example Sources:** Images derived from malware files supplied by Comodo Inc, converted to RGB using the bin2png script.

<https://web.cs.hacettepe.edu.tr/~selman/malevis/>

Incremental Training Dataset

DIKE DATASET

- **Features:** The DikeDataset includes benign and malicious PE and OLE files, with labels indicating malice levels and malware family membership.
- **Purpose:** Designed for AI training, it supports machine learning and deep learning models to predict a file's malice and classification.

<https://github.com/iosifache/DikeDataset?tab=readme-ov-file#description-%EF%B8%8F>

Training Dataset: Raw PE as Image

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
1	hash	pix_0	pix_1	pix_2	pix_3	pix_4	pix_5	pix_6	pix_7	pix_8	pix_9	pix_10	pix_11	pix_12	pix_13	pix_14	pix_15	pix_16	pix_17	pix_18
2	b324140e	15	15	239	15	223	36	102	243	102	102	254	36	40	7	102	92	15	15	
3	1d32b132	234	196	8	20	182	56	27	223	144	255	207	0	77	81	112	176	131	222	
4	e44fea491	196	255	5	97	35	112	219	189	217	66	36	90	117	0	69	217	132	221	
5	95badb16	232	252	183	39	51	1	255	87	94	128	69	252	255	236	0	150	80	116	
6	f30f32a4f4	81	84	204	228	255	157	76	254	128	39	79	255	0	255	48	0	80	0	
7	5a7c0331a	238	158	107	2	102	94	16	133	144	137	1	178	206	57	7	61	123	73	
8	449a7d280	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
9	e5bf0a922	8	219	133	55	96	93	21	230	136	67	26	65	82	170	84	71	161	187	
10	3965b3eca	248	0	247	211	247	216	202	34	202	34	202	34	0	0	0	0	0	0	
11	72e66c0d6	77	0	0	106	104	192	36	12	2	36	141	139	80	240	0	194	10	80	
12	024363efa	89	64	76	87	126	190	11	231	60	45	237	43	47	142	7	93	203	7	
13	4563136d1	47	0	0	0	0	64	0	0	0	0	0	0	0	0	0	0	0	0	
14	c3d69f32c	64	195	0	80	0	200	139	51	84	210	80	232	255	255	255	141	0	131	
15	7b5f7f463	254	255	255	0	31	38	232	255	157	0	92	255	255	255	254	240	254	89	
16	200834c53	96	104	0	3	216	131	255	2	128	48	69	30	157	157	72	113	0	11	
17	b66de013b	204	197	236	141	64	229	137	139	0	232	137	236	204	178	0	125	0	82	
18	5b7473744	0	36	69	3	0	0	0	128	0	0	0	0	0	69	193	80	16	117	

raw_pe_images +

Why did we chose this dataset?

We selected this dataset primarily because it offers 32x32 greyscale images, which can be readily inputted into our CNN (Convolutional Neural Network) model.

Pre Processing of Raw PE images

Imbalanced classes

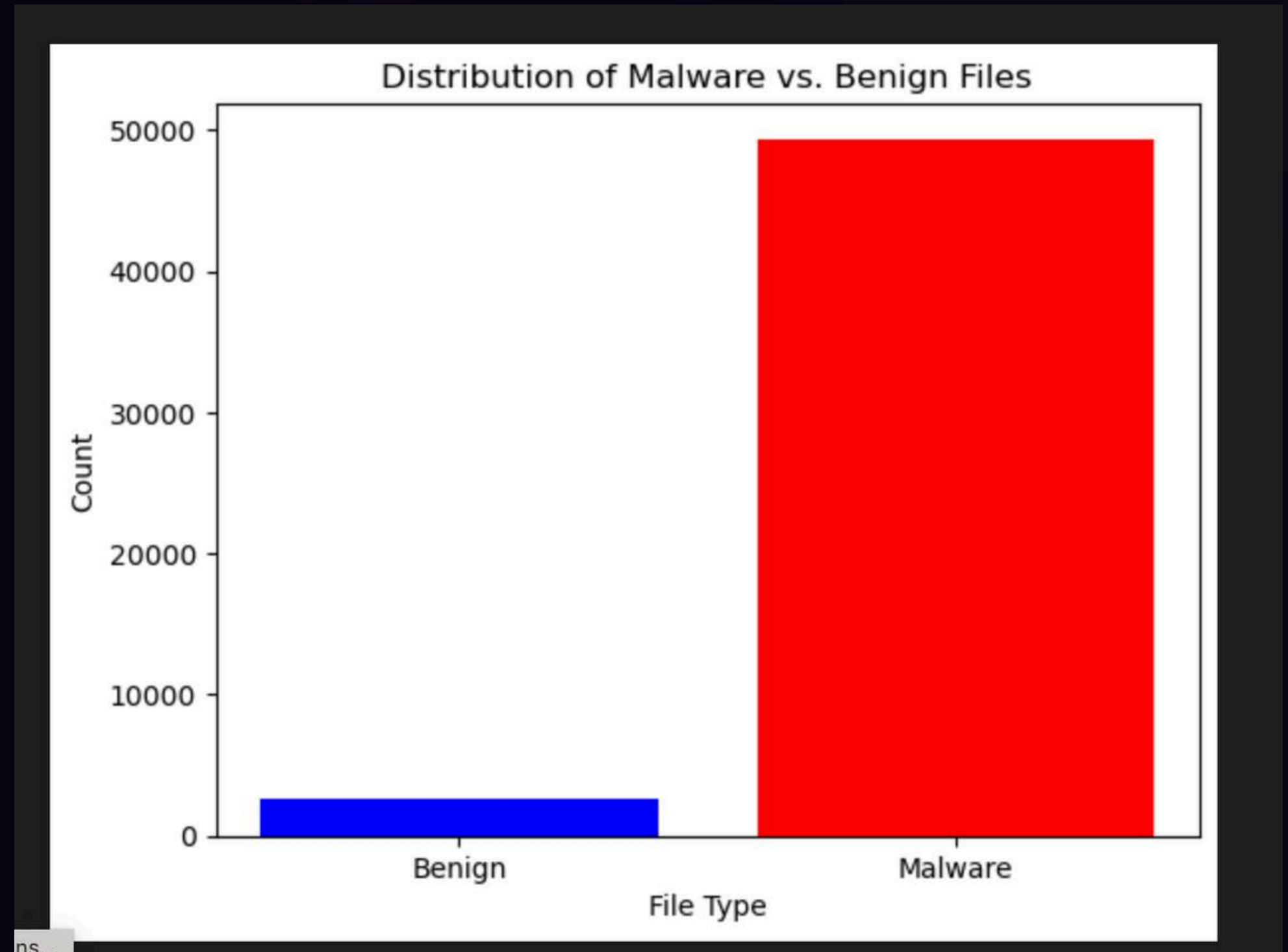
Most of the datasets we gathered from various sources showed a skewed distribution of classes.

Such an issue can lead to:

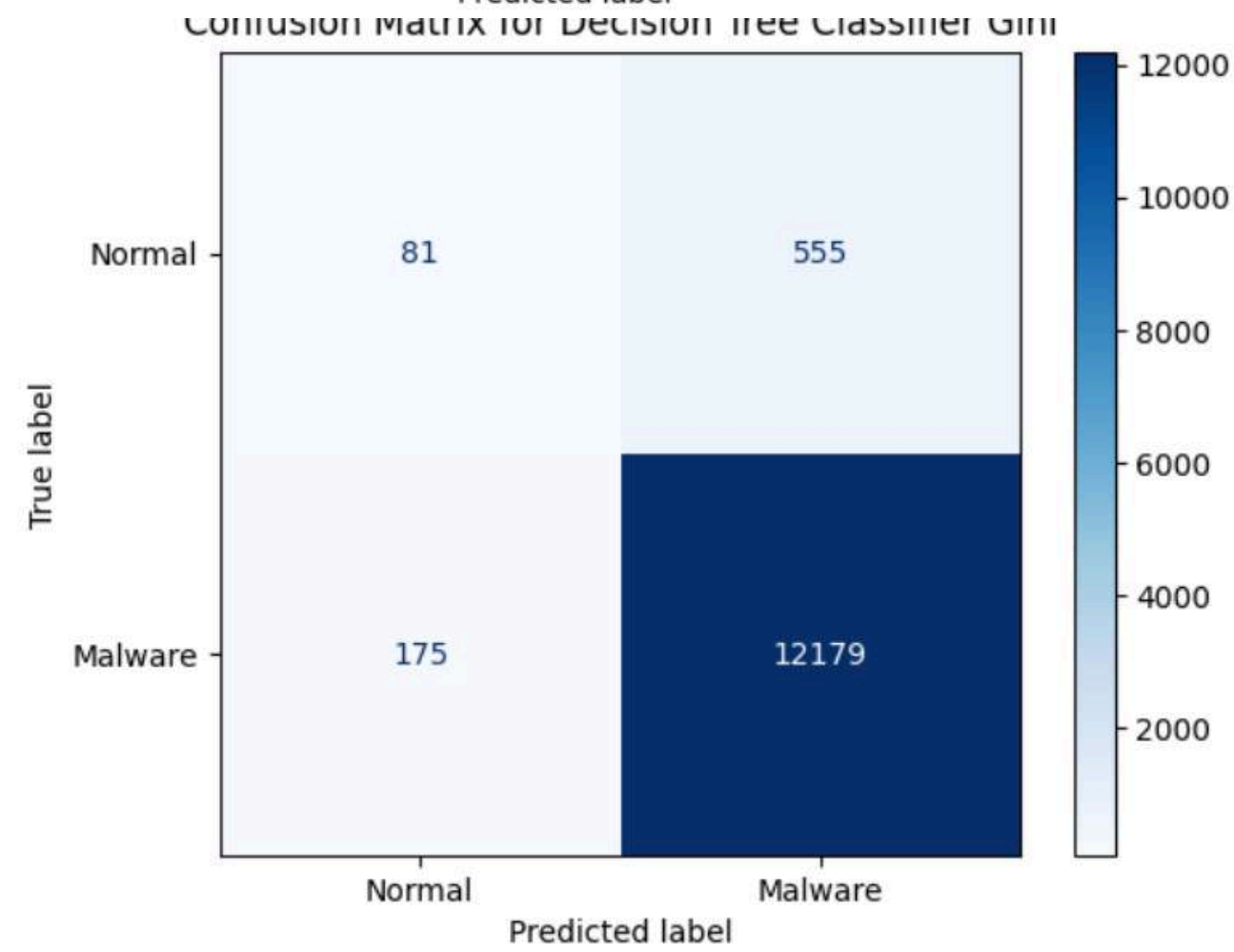
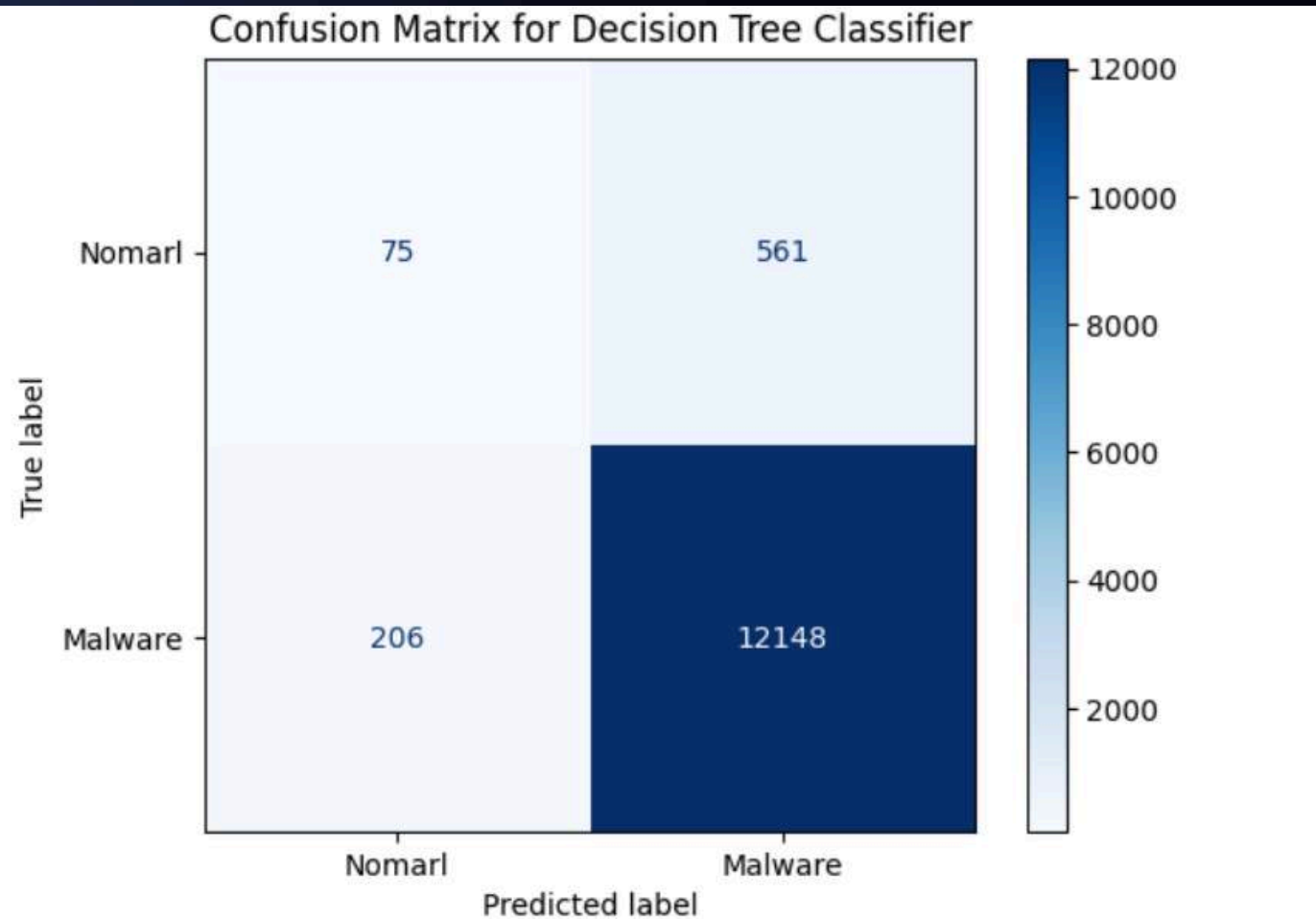
1. Model Bias Towards Majority Class
2. Poor Generalization Over Minority Class
3. Evaluation Metrics Become Misleading

SMOTE

- We used SMOTE (Synthetic Minority Over-sampling Technique) to create synthetic samples based on existing minority instances, helping to balance the dataset without losing valuable data.



Benchmark dataset: Raw PE as Image



Algorithms: Decision Tree with Gini criterion & Entropy criterion.

Accuracy for Gini Criterion Model:

a. Validation Set: 94.38%

a.

b. Training Set: 96.78%

b.

Accuracy for Entropy Criterion Model:

a. Validation Set: 94.10%

a.

b. Training Set: 96.74%

b.

F1 Score for Gini Criterion Model:

a. For class 'Malware': 0.97

a.

b. For class 'Non-Malware': 0.18

b.

F1 Score for Entropy Criterion Model:

c. For class 'Malware': 0.97

c.

d. For class 'Non-Malware': 0.16

d.

Their model perform exceptionally well in identifying 'Malware', they struggle with 'Non-Malware' classes, indicating possible issues with class imbalance or model overfitting.

Bechmark Dataset: Malvis



Bechmark:

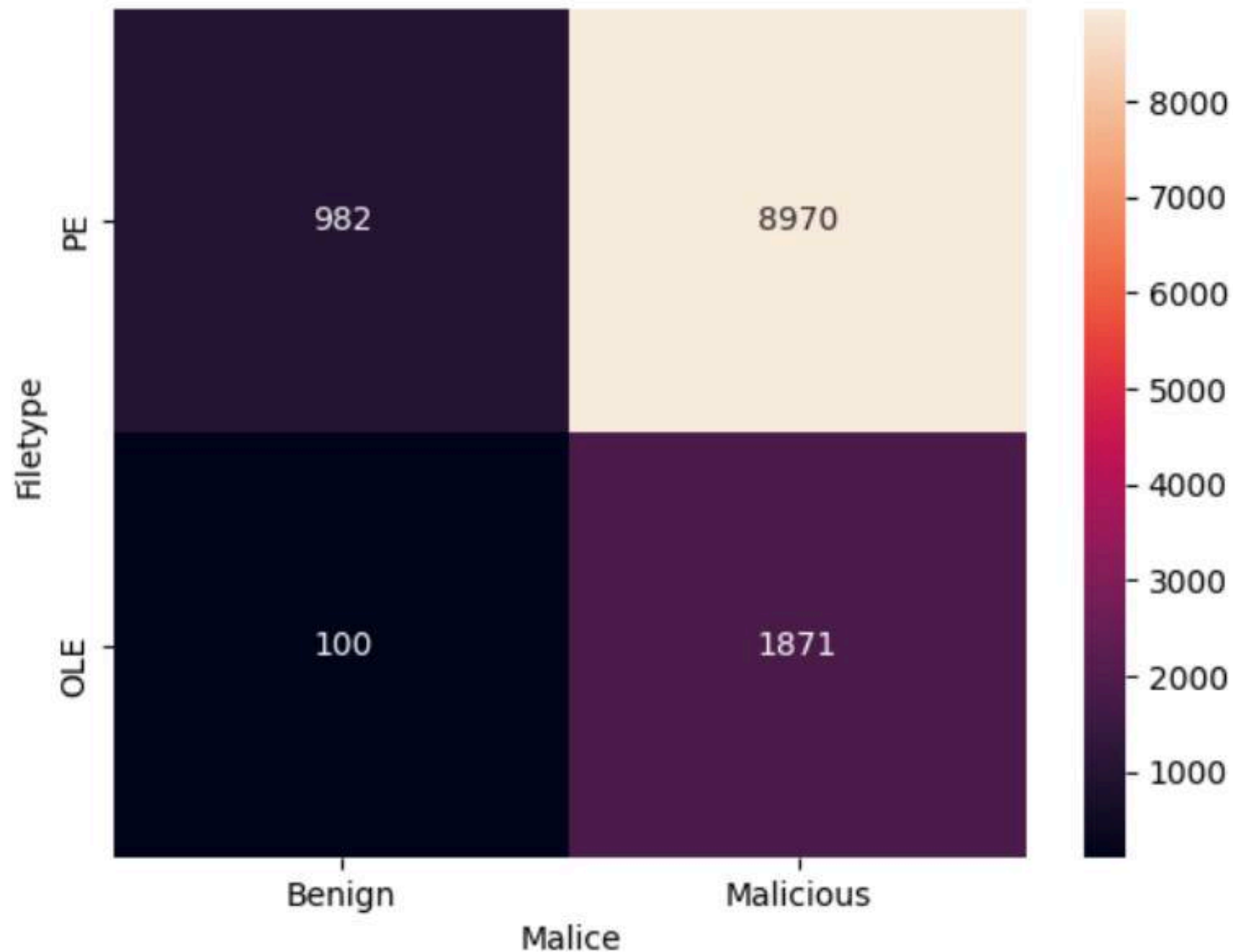
DenseNet: Achieved the top accuracy of 97.48% using RGB images, outperforming other models tested.

ResNet18: Recorded a strong accuracy of 97.18% and demonstrated high efficiency, processing 3,644 images in just 5 seconds.

Other CNNs: Models like VGG, AlexNet, and Inception were also tested, but DenseNet and ResNet provided the best results.

Dataset: 8,750 training and 3,644 test instances across 25 classes, derived from malware files.

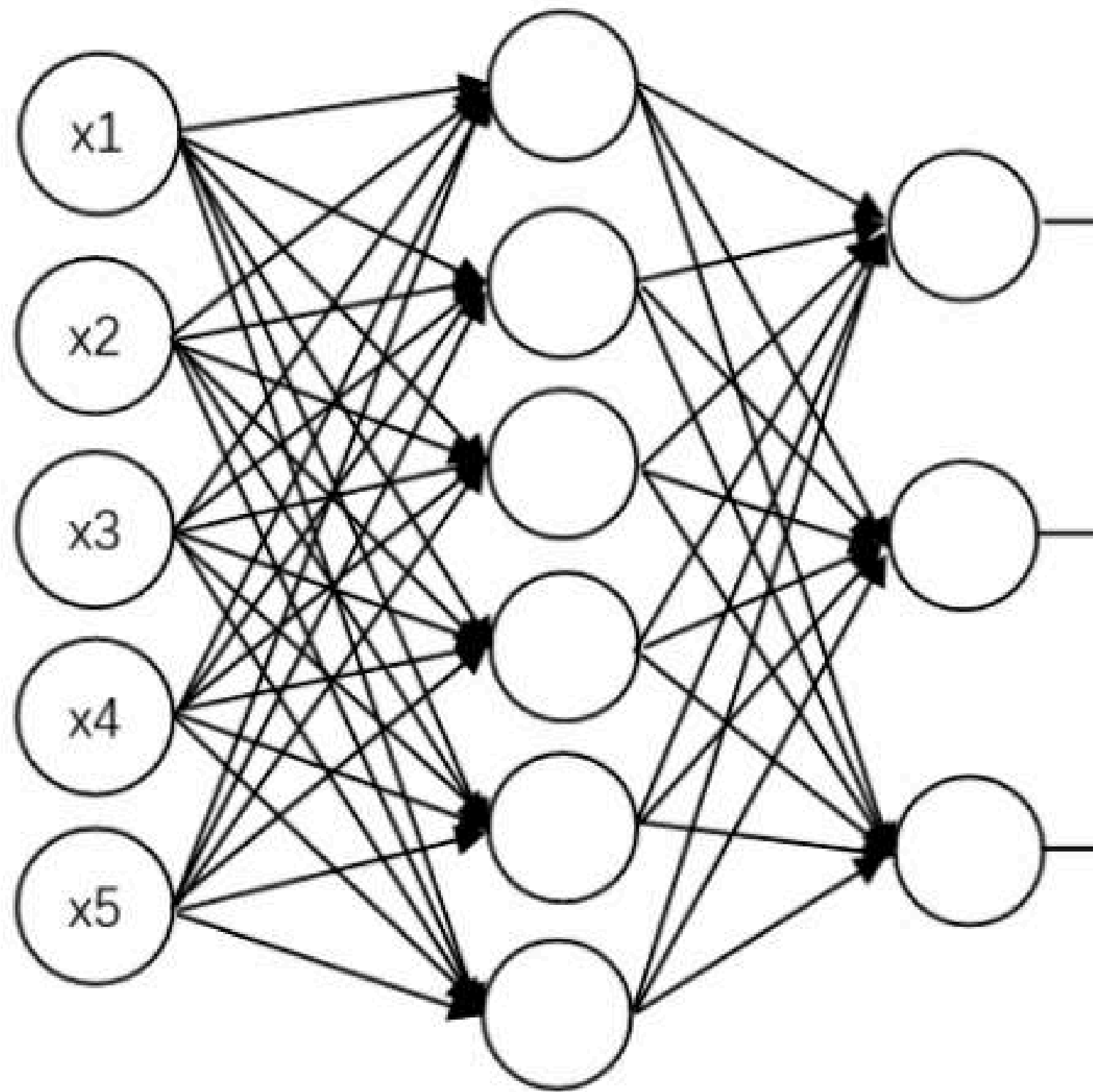
Training Dataset: Raw PE as Image



Why did we chose this dataset?

We selected this dataset for our ML model's incremental training because it offers a diverse mix of benign and malicious PE and OLE files. The substantial variance in file types and malice levels, as shown in the heatmap, ensures a rich training environment that enhances our model's accuracy and adaptability to new data.

ML Methodology



Convolutional Neural Networks (CNN) + LSTM

CNN with LSTM solves the problem stated.

CNN & LSTM

Comparing CNN with ordinary machine learning it can be said that:

- CNN in malware image classification improves the accuracy of malware classification
- Reduces the time needed for classification.

Advantage 1

Adaptability to Various Malware Types

The CNN-LSTM model's flexible architecture makes it suitable for detecting a wide range of malware types, from viruses and worms to more sophisticated ransomware and spyware, by learning their unique spatial and temporal characteristics.

Advantage 2

Automated Feature Learning

One of the biggest challenges in malware detection is feature engineering, i.e., selecting and designing the right features for detection algorithms. The CNN-LSTM architecture can automatically learn and select relevant features from raw data, reducing the need for manual feature engineering and making the model more adaptive to evolving malware techniques.

Traditional ML

4) Logistic Regression: The log loss test of Logistic regression algorithm is 1.3985948869851592

3) KNN: The log loss test of KNN algorithm is 0.44410209290437647

5) Random Forest: The log loss test of random forest algorithm is 0.1770150574797033

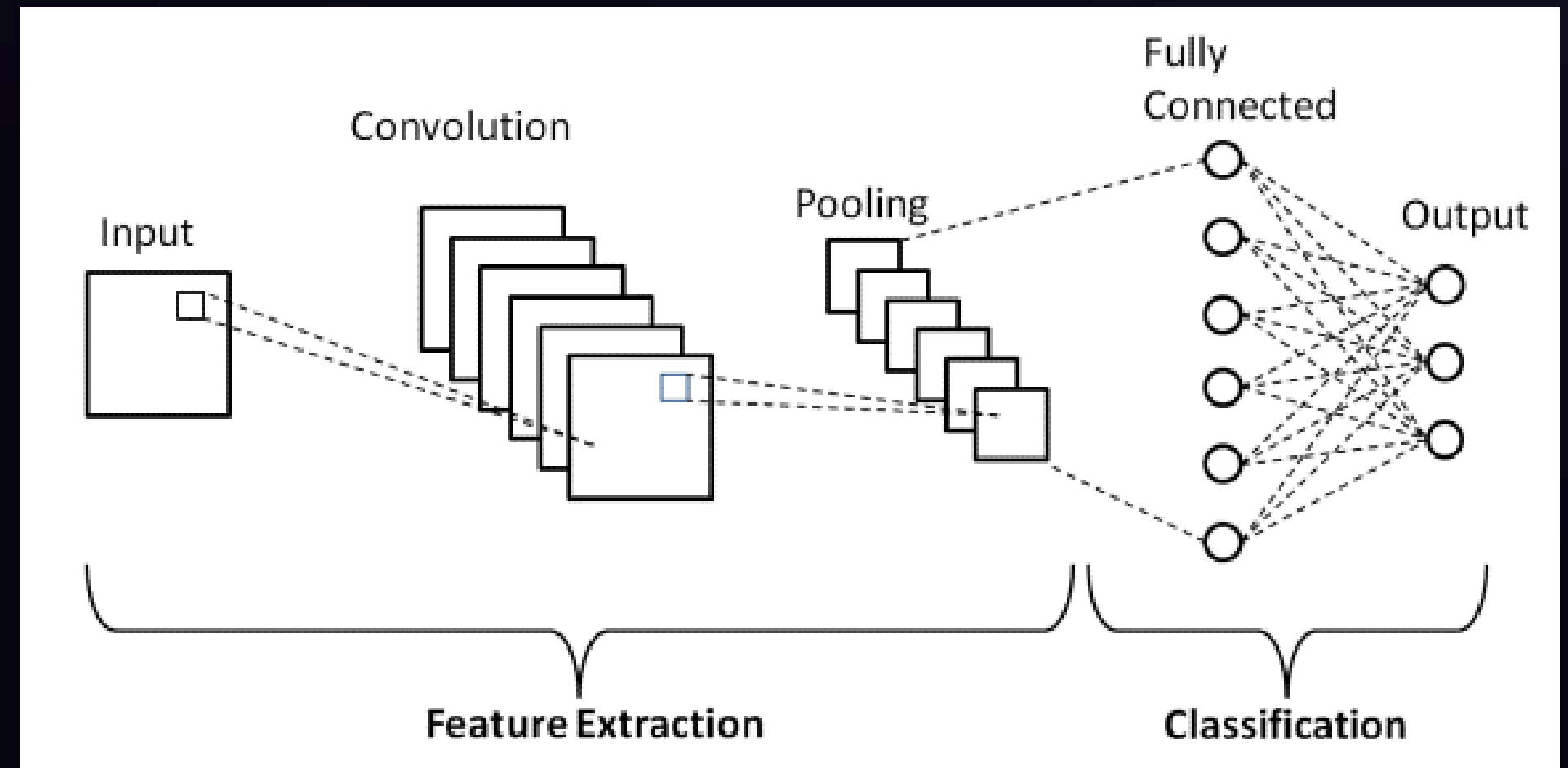
CNN & LSTM

Advantage 3

High Performance

Integration of CNN and LSTM models for malware detection leverages the strengths of both architectures, providing a powerful tool for identifying malicious software with high accuracy, efficiency, and adaptability to new threats. Some research papers promising up to 99% accuracy.

- Convolutional layer
- Pooling layer
- Fully connected layer



Multi Layer Feedforward Networks

- This type of network has one or more hidden layers except for the input and output. Its role is to intervene in data transfer between the input and output layer.

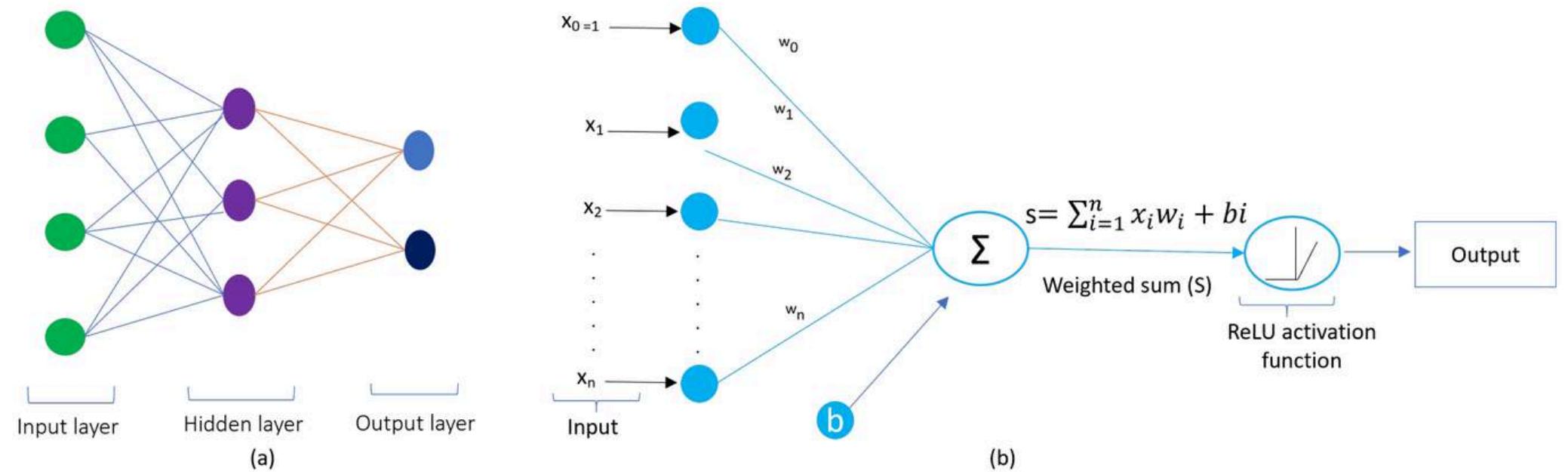
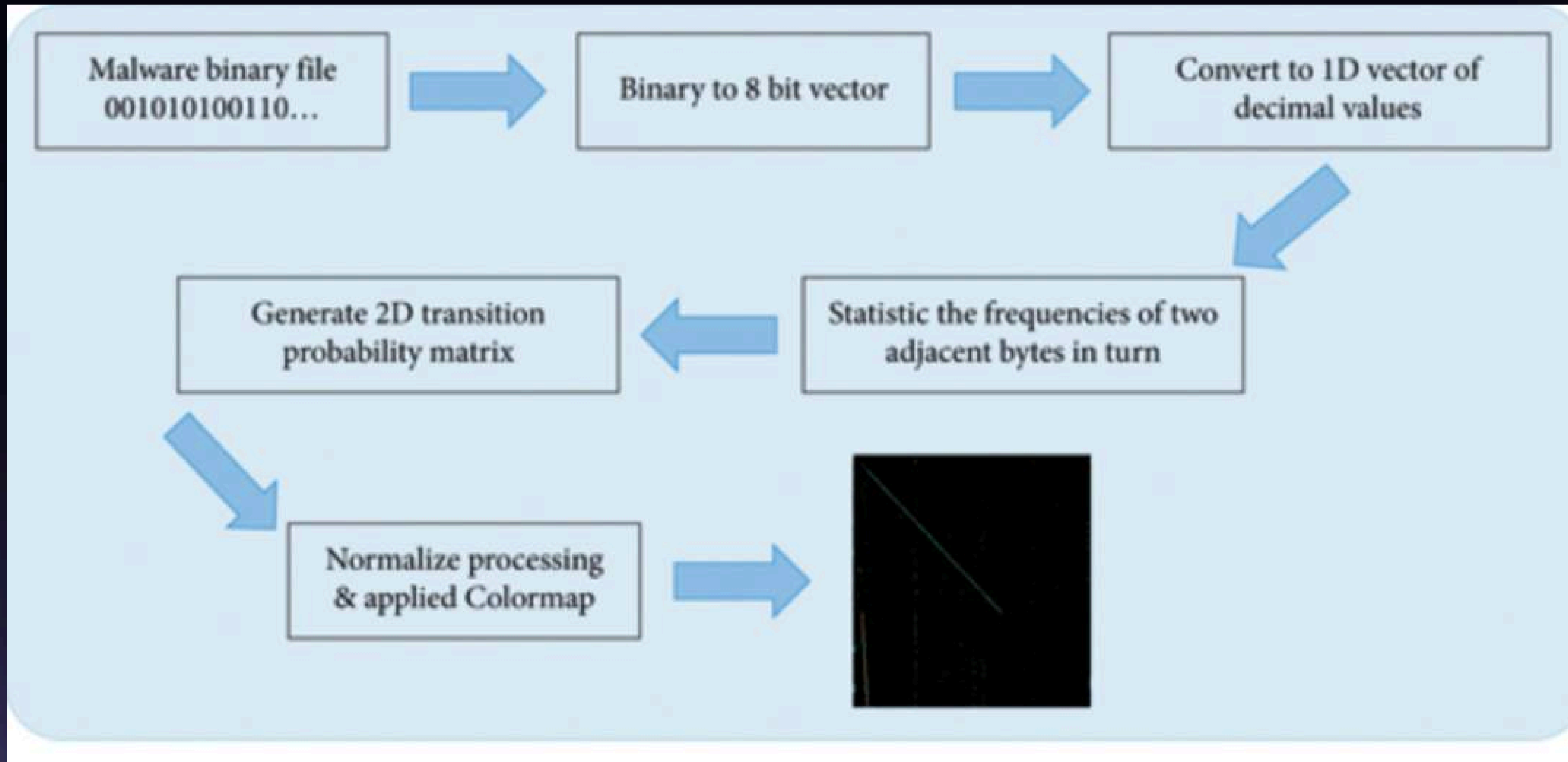
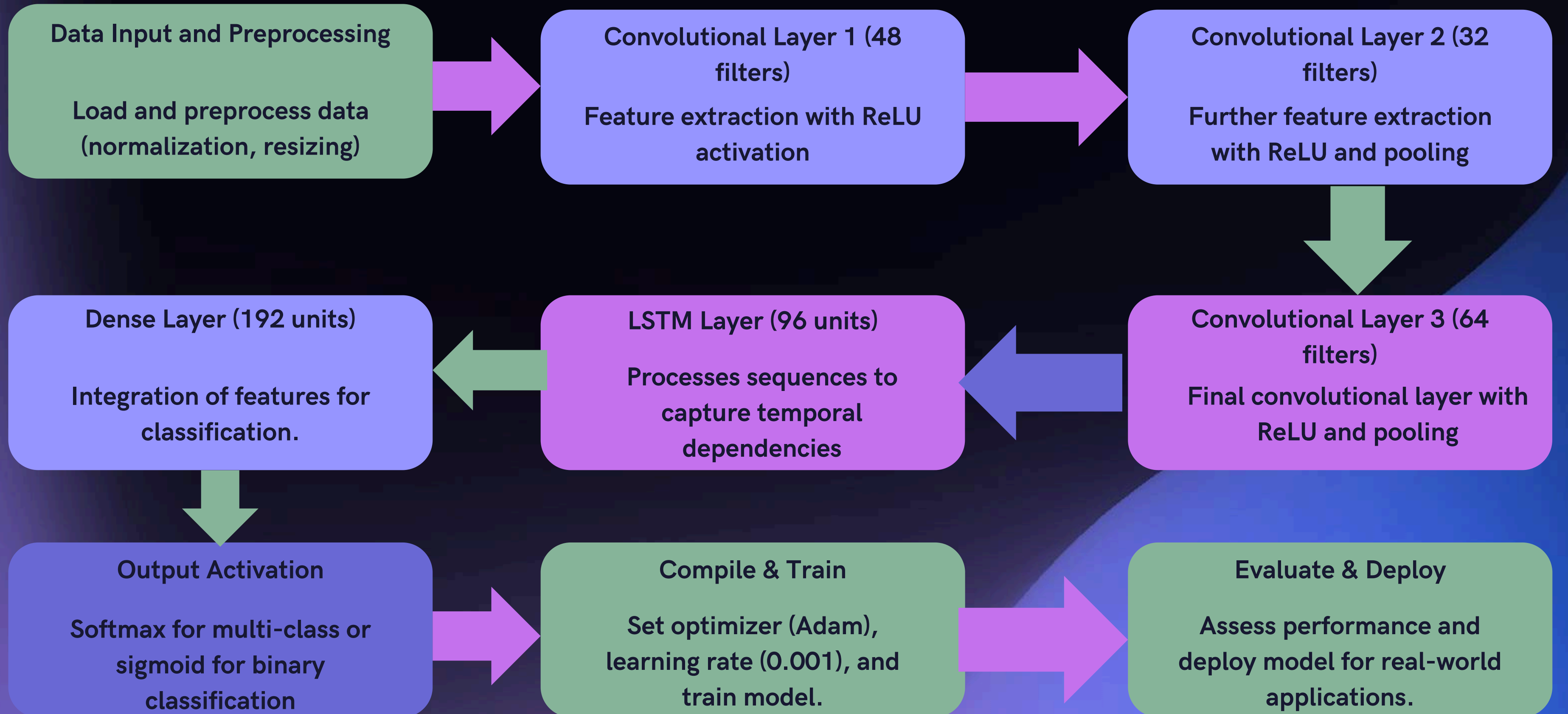


Figure 2: An example of (a) A simple architecture of an artificial neural network (b) Illustration of activation operation in artificial neural network using ReLU activation function

Conversion of malware to image for CNN



CNN & LSTM Architecture



Model & Performance Matrix

Classification Report:

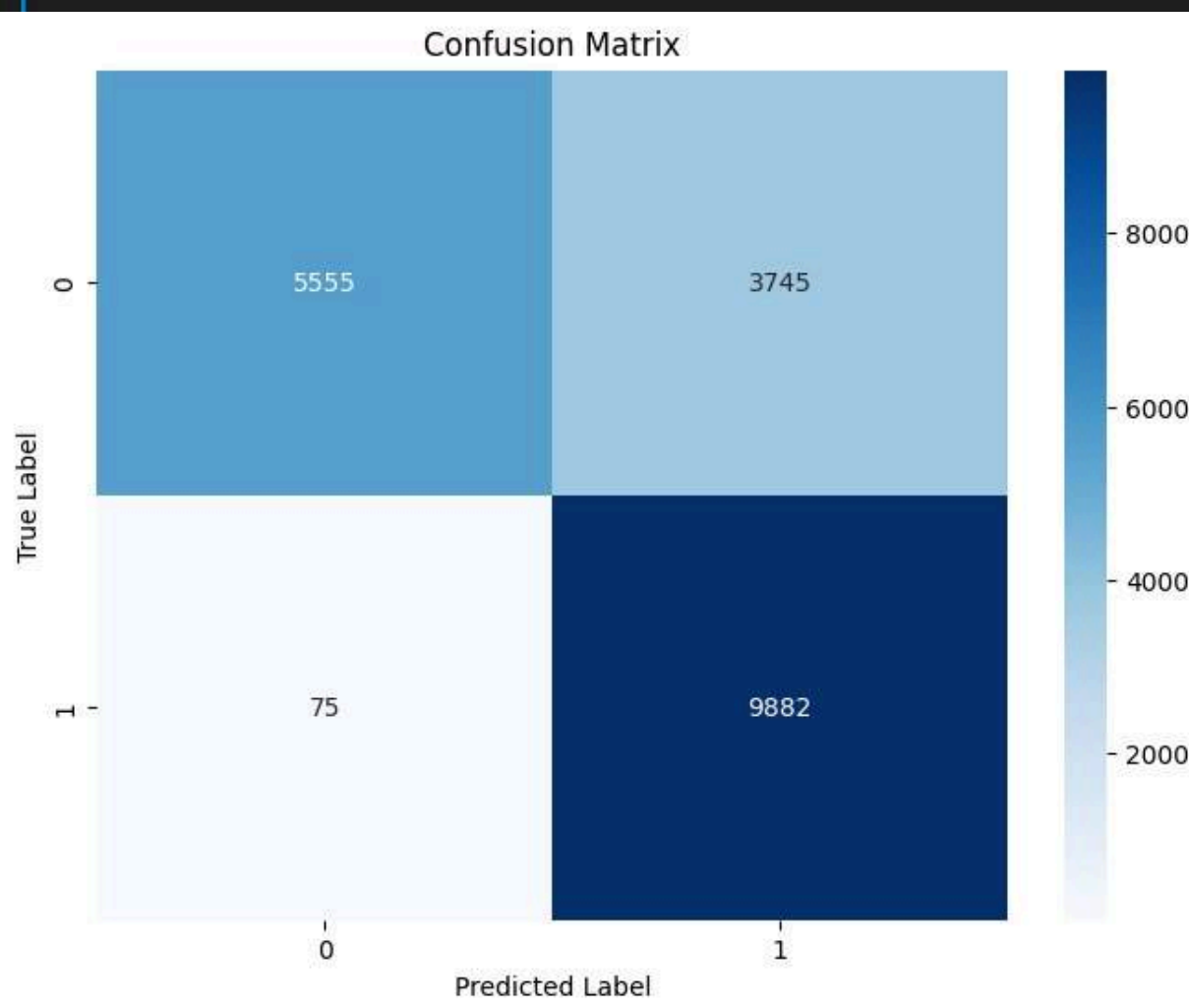
	precision	recall	f1-score	support
0	0.99	0.67	0.80	9300
1	0.76	0.99	0.86	9957
accuracy			0.84	19257
macro avg	0.88	0.83	0.83	19257
weighted avg	0.87	0.84	0.83	19257

Class 0 Performance: High precision (0.99) but lower recall (0.67) indicates effective non-threat identification with some missed detections.

Class 1 Performance: Excellent recall (0.99) captures almost all malicious instances, though precision at 0.76 points to a moderate rate of false positives.

Confusion Matrix for Class 1: Effectively identifies 9882 malicious instances with minimal misses (75 false negatives), demonstrating robust threat detection.

Confusion Matrix for Class 0: Correctly classifies 5555 non-malicious instances but with a high number of false positives (3745), suggesting a need to reduce false alarms.



Model Hyperparameter Tuning

Convolutional Layers:

- First convolutional layer with 48 filters.
- Second convolutional layer with 32 filters.
- Third convolutional layer with 62 filters.

Learning Rate: Set at 0.001.

Optimizer: Utilizes the Adam optimizer for efficient training.

LSTM Layer: Integrated to process sequential data and capture long-term dependencies.

Dense Layer:

Includes a dense layer with an activation function set to sigmoid, ideal for binary classification tasks.

Batch Size and Epochs: Configurable settings for training not directly provided but essential for the model's training process.

This setup details the tuned hyperparameters and the structured layering of your CNN-LSTM model, emphasizing its capacity for feature extraction and sequential data processing.

Deployability & Future Scope

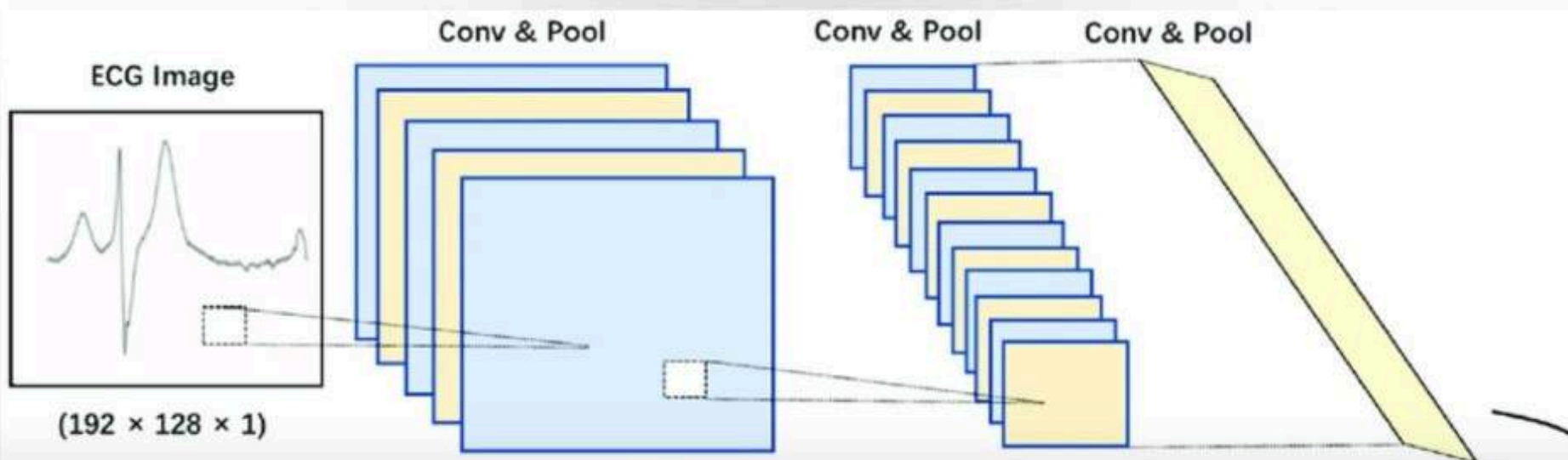
127.0.0.1:5000

MLPR

Cutting edge *Malware* Detection Model

Find accurately using our ML Model, based on CNN-LSTM architecture whether the executable file you are going to run is malicious or not.

[Request Demo](#) [Try for Free](#)



The diagram illustrates the model's architecture. It starts with an 'ECG Image' of size $(192 \times 128 \times 1)$. This is followed by three sequential 'Conv & Pool' stages. The first stage produces a stack of feature maps. The second stage further processes these into a stack of smaller feature maps. The final stage leads to a single output layer of size $(64 \times 64 \times 64)$.

We have successfully deployed our model locally with a front-end interface and plan to demonstrate a demo.

Our future scope for this project includes:

- Implementing dynamic analysis, as currently the model uses static analysis.
- Working with larger datasets and more real-time, industry-aligned data to further enhance our model's capabilities and efficiency.
- Upgrading our model to make it product-ready for launch in the enterprise technology market.

References

References for literature survey:

Zheng, W., & Omote, K. (2021). Robust Detection Model for Portable Execution Malware. IEEE International Conference on Communications.
<https://doi.org/10.1109/ICC42927.2021.9500440>

Dasari, H., Danduboina, B. P., Chinna Rao, M., & IJIRT. (2022). Malware Prediction Classifier using Random Forest Algorithm. In International Journal of Innovative Research in Technology (Vol. 9, Issue 2, pp. 108–109) [Journal-article].
https://ijirt.org/master/publishedpaper/IJIRT155843_PAPER.pdf

Zheng, W., & Omote, K. (2021). Robust Detection Model for Portable Execution Malware. IEEE International Conference on Communications.
<https://doi.org/10.1109/ICC42927.2021.9500440>

Stay Tuned!

...