Malware Detection and Classification in IoT Devices using Deep Learning

Guided By:
Mrs. Sanjukta Mohanty

Presented By:
Sarthak Shukla (Regd No:- 2111100404)
Kumar Santosh (Regd No:-2111100406)
6th Semester
B.Tech,CSE

Contents

INTRODUCTION

- It is a system that detects and classifies the malware using Deep Learning techniques like CNN, Ensemble learning.
- The integration of deep learning techniques in IoT devices offers a promising approach to effectively identify and mitigate malware threats, ensuring the security and integrity of interconnected systems in the evolving AI world.
- It is used to classify the malware as per its class by taking input as grayscale image of byte file.

Literature Survey

Sl. No.	Author Details	Objective	Key Description	Limitations
1	Rajasekhar Chaganti et al. [3],2022	The Paper proposed a Deep Learning based Bidirectional-Gated Recurrent Unit Convolutional Neural Network (Bi-GRU-CNN) model to detect the IoT malware and classify the IoT malware families using Executable and Linkable Format (ELF) binary file byte sequences as an input feature.	The approach proposed by the paper obtained 98% accuracy for IoT malware detection case and 98% for IoT malware family classification.	Imbalanced datasets. Unexplored adversarial attacks
2	Zhongru Ren et al. [5], 2020	The paper introduces two groundbreaking deep learning methods (DexCNN, DexCRNN) for Android malware detection, featuring an end-to-end learning process that surpasses existing techniques.	The proposed methods can achieve 93.4% (DexCNN) and 95.8% (DexCRNN) detection accuracy respectively for benign and applications	Limited input: The proposed methods only analyze the classes.dex file within Android APKs, neglecting other valuable information in other files like AndroidManifest.xml.
3	Farhan Ullah et al. [7], 2019	The paper proposed a combined deep learning approach to detect the pirated software and malware-infected files across the IoT network.	The experimental results show that the combined approach retrieve maximum classification results as compared to the state of the art techniques.	Tokenization extracts keywords but misses information about internal code structure
4	Saddam Hussain Khan et al. [8], 2023	The researcher developed a new malware detection framework, Deep Squeezed Boosted and Ensemble Learning (DSBEL), comprised of novel Squeezed-BoostedBoundary-Region SplitTransform-Merge (SB-BR-STM) CNN and ensemble learning.	The adopted method has a progressive performance as 98.50% accuracy, 97.12% F1-Score, 91.91% MCC, 95.97 % Recall, and 98.42 % Precision	Lack of Zero-Day Attack Testing.Dataset Scope: The evaluation used only a limited no. of Dataset.

Sl. No.	Author Details	Objective	Key Description	Limitations
5	Adel Abusitta et al. [6], 2022	The paper proposed a deep learning-powered anomaly detection for IoT that can learn and capture robust and useful features, which cannot be significantly affected by unstable environments.	Experimental results based on real-life IoT datasets show the effectiveness of the proposed framework in terms of enhancing the accuracy of detecting malicious data compared to the other models.	Imbalanced Dataset.
6	Vinayakumar, R. et al. [3], 2019	The approach involves a three-pronged strategy: checks both classical and deep learning models, removes bias from training data, and uses a new image processing technique.	Deep learning beats traditional methods in malware detection. This approach works across operating systems and packing formats, and is faster than traditional analysis. The core module, DIMD, using CNN-LSTM achieved 96.3% accuracy and has potential for further improvement with more complex architectures.	The limitation of this work is that a detailed analysis on the hyper parameter tuning method has not been adopted for the variants of the existing deep learning architectures
7	Anandharaju et al.	The paper discusses feature representations, extraction techniques, and machine learning models used. It highlights practical challenges and potential future research directions in this field.	Graph-based methods show potential but need to meet IoT resource requirements.	Zero-day attacks and concept drift in machine learning models.Wide variety of malware families, OS platforms, and CPU architectures.
8	Omer Aslan et al.[5], 2021	Proposed deep learning architecture effectively detects and classifies malware variantsHybrid approach with pre-trained networks and transfer learning is used.	Proposed method outperforms state-of-the-art methods in terms of accuracy.The proposed method achieves high accuracy in classifying malware variants	Performed with limited computer power and resources. Increasing hidden layers increases performance up to a certain level.

Sl. No.	Author Details	Objective	Key Description	Limitations
9	Rajasekhar et al.[3], 2023	It proposes a CNN model for classifying malware in PE binary files. The model achieves an accuracy of 97% using fusion feature sets.	The proposed CNN model achieved a malware classification accuracy of 97%. The CNN model outperformed the SVM model in accurately classifying malware samples.	Adversarial attacks on ML or DL models can impact malware classification performance.
10	Elayan et al.[3], 2021	It proposes a novel method using a deep learning technique called Gated Recurrent Unit (GRU) to detect malware in Android application.This method analyzes Android app behavior (API calls & permissions) using a GRU model trained on an app dataset(CICAndMal2017) to detect malware.	The model obtained accuracy of 98.6% as compared to traditional methods.	GRU models can be complex and their decision-making might be unclear.

Problem Statement

- Unable to work on imbalance datasets and detect unexplored adversarial malware attacks.
- Unable to prevent zero day attacks due to use of primitive methods such as Black listing.
- Taking one parameter(only accuracy) to check the performance of the overall model.

Motivation

Malware detection efforts contribute to the reduction of cybercrime rates by identifying, isolating, and neutralizing malicious software used in cyberattacks.

This research project help mitigate financial losses caused by cyberattacks by providing early detection and response mechanisms.

It is vital to the security of key infrastructure sectors such as energy, transportation, healthcare, and telecommunications. Preventing malware assaults on critical systems and networks helps to maintain the continued and dependable functioning of key services on which society relies on a daily basis.

Objective

- **Machine Learning and Deep Learning Techniques:** Utilizing techniques like pre-trained CNN architecture to extract relevant features from dataset for multi classification.
- **Semi-Balanced Dataset Creation:** Merging diverse datasets and potentially applying oversampling or undersampling techniques to address data imbalance.
- **Beyond Blacklisting:** Moving beyond static blacklisting towards a dynamic classification system that can identify novel malware based on its behavior and features.

Proposed Methodology

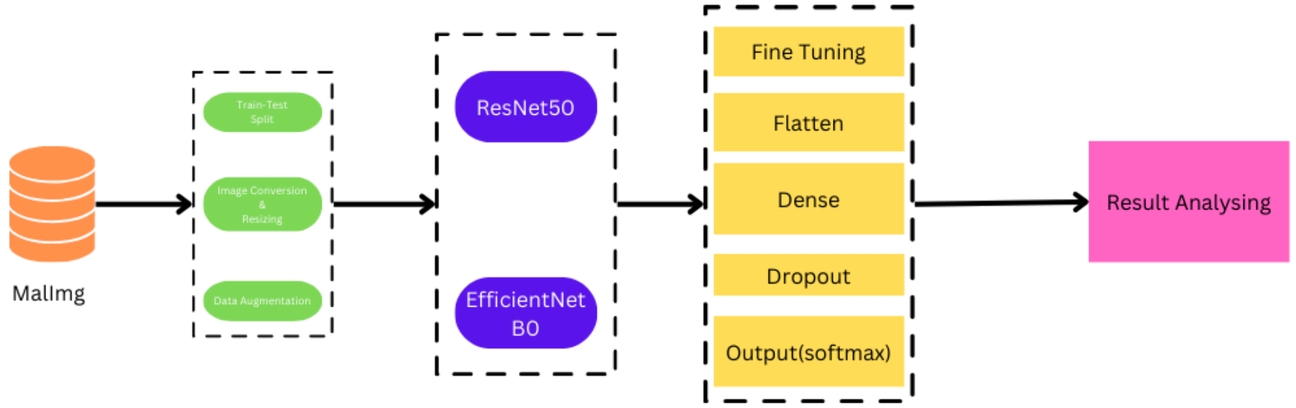

Fig.1 Flow diagram of MalImg Dataset

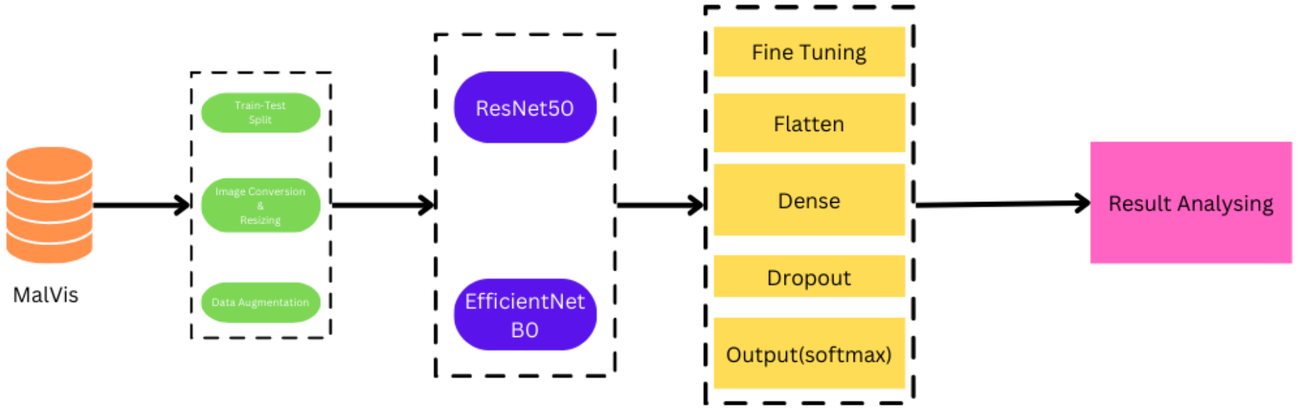

Fig.2 Flow diagram of MalVis Dataset

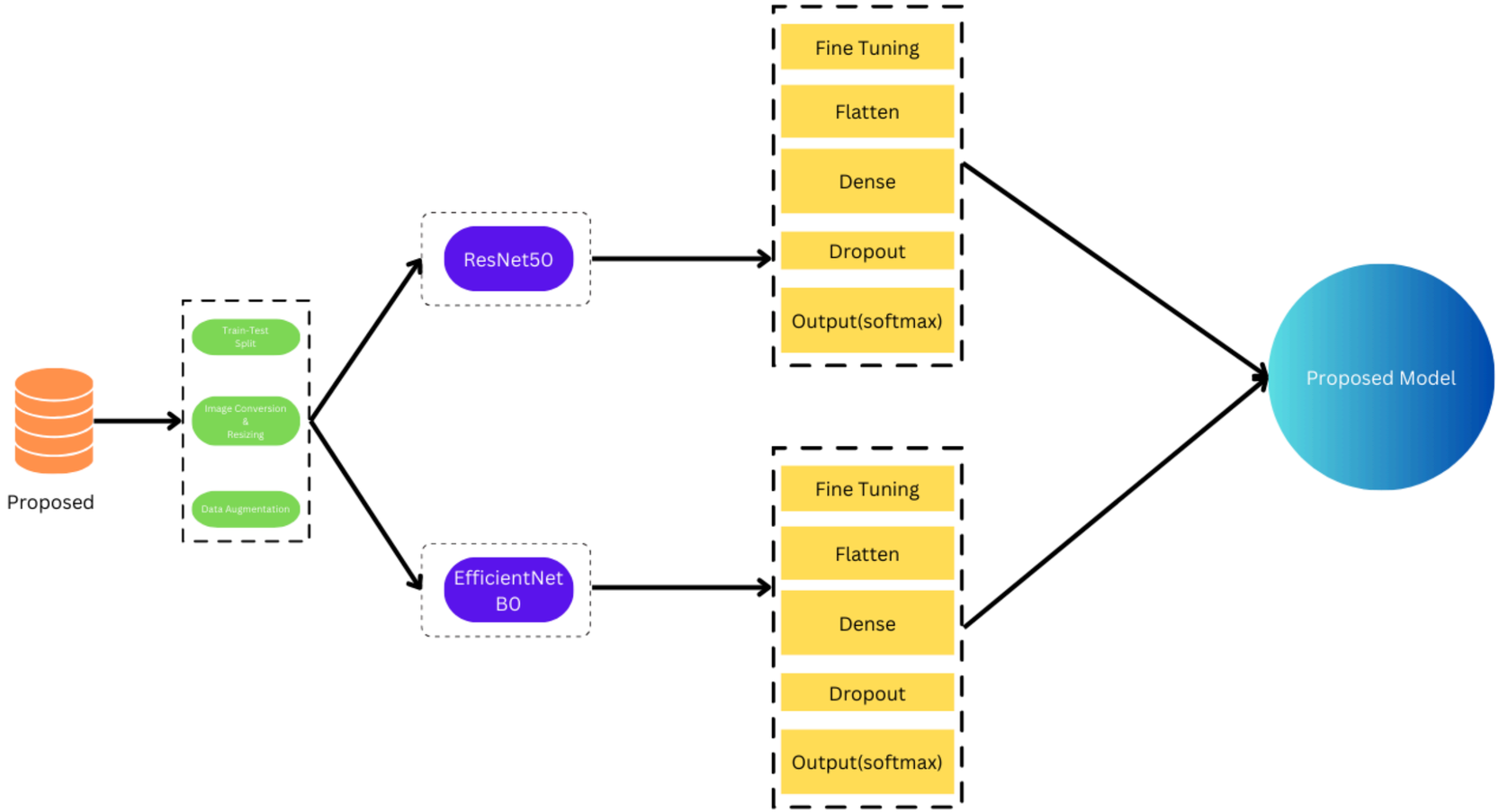

Fig.3 Flow diagram of Proposed Dataset

Datasets

Table 1. Dataset-1 characteristics

Data Set	Number of Images	Number of classes
MalImg	9339	25

- The dataset(MalImg) consist of gray scale images.It is imbalanced dataset.

Table 2. Dataset-2 characteristics

Data Set	Number of Images	Number of classes
MalVis	9100	25

- The Dataset(MalVis) is a balanced Dataset. It consist of RGB images.

Table 3. Proposed dataset characteristics

Data Set	Number of Images	Number of classes
Proposed Model	9868	31

- Proposed dataset is a Semibalance dataset.

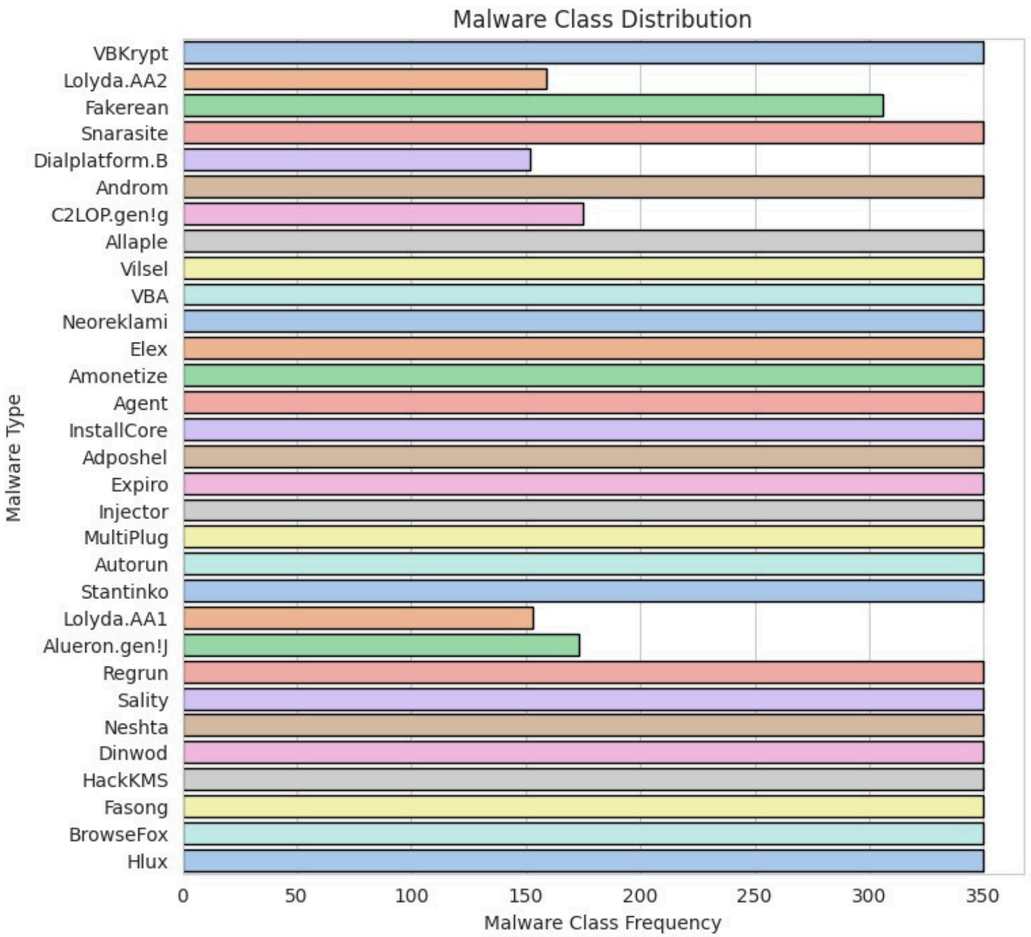

Fig.4 MalVis Dataset

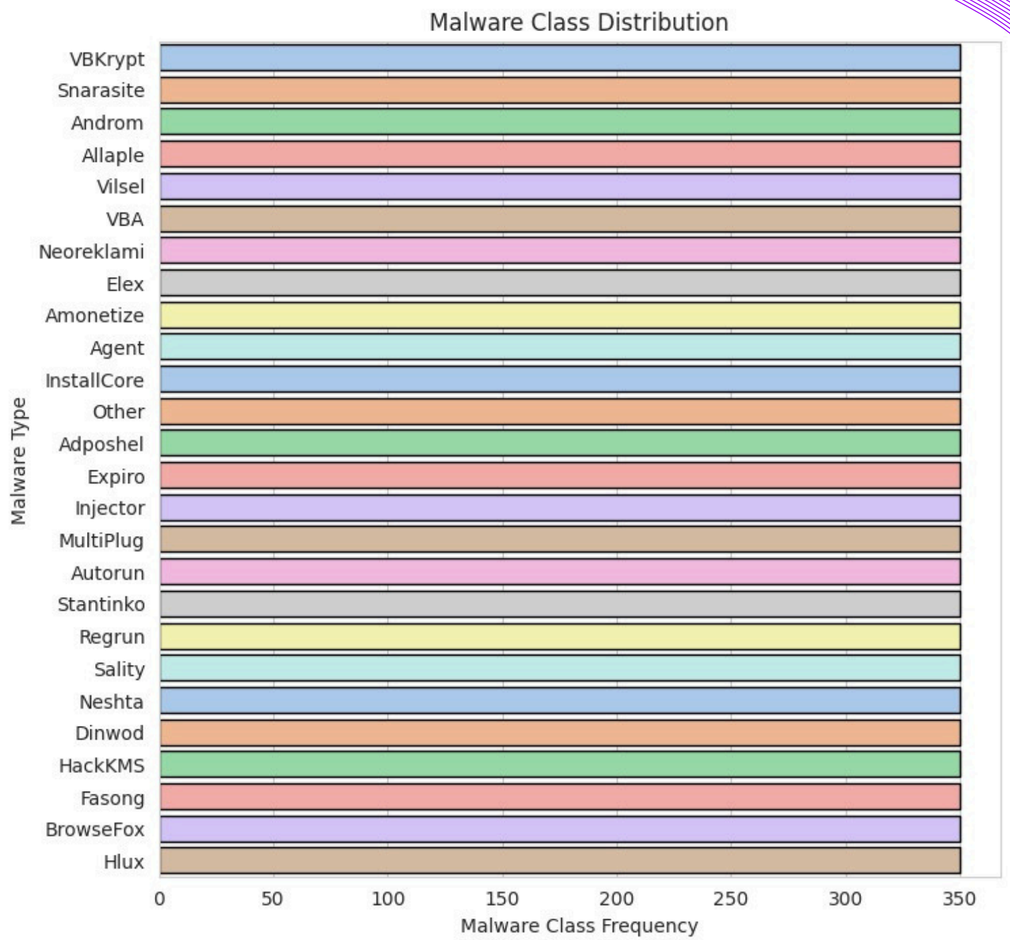

Fig.5 Proposed Dataset

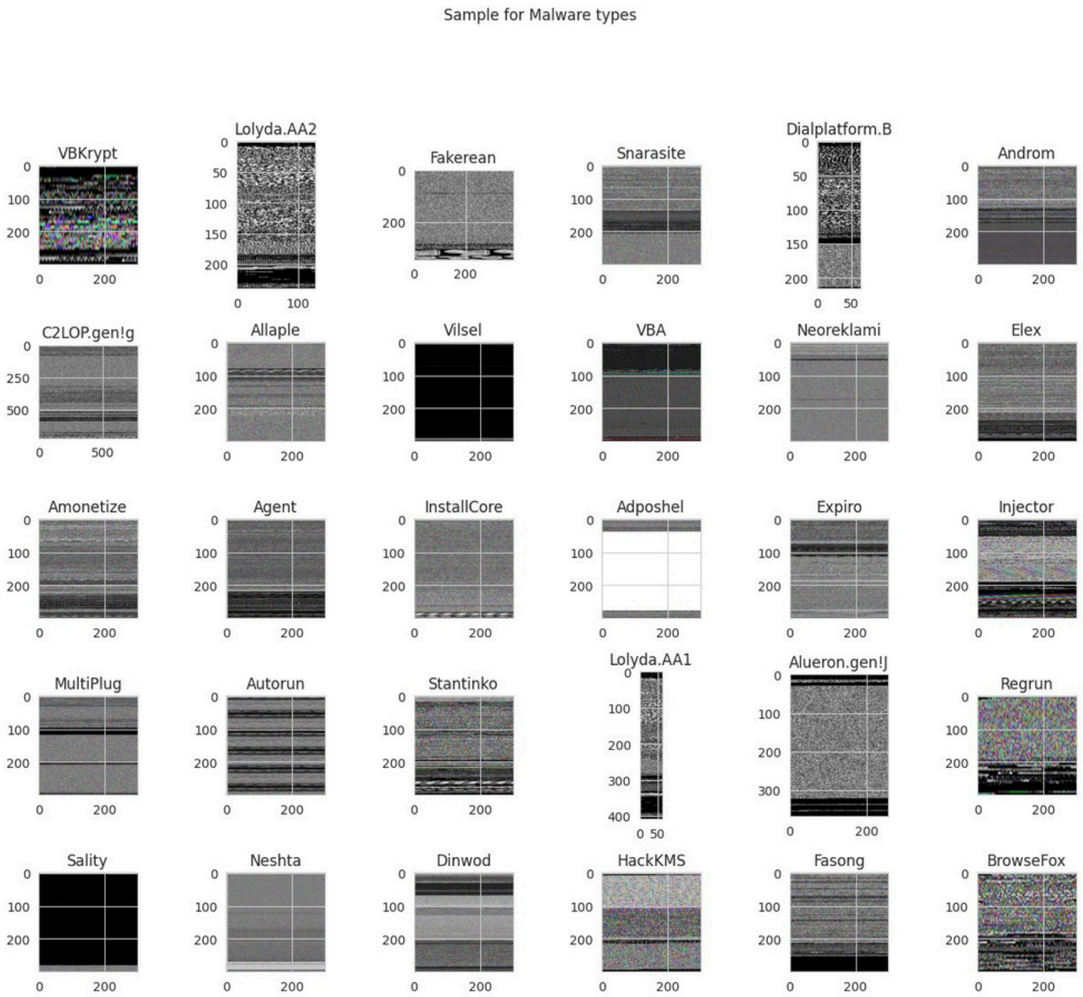

Fig.6 Sample Malware types

Image Preprocessing

- In the dataset, it is already provided the visualization of executable malware binary files. The main aim is to visualize binary files as a grayscale image.
- The Proposed dataset includes both RGB and grayscale photos. Additionally, every image in the MalImg dataset has a distinct size, which needs to be combined into one image size. All of the photos are converted to RGB and scaled to 75 by 75.
- Data Augmentation is also done to address the problem of data imbalance by enabling to produce several copies of the same data from various perspectives.For data augmentation and picture pre-processing, we also employed Keras Image Data Generator. In order to flip a picture, Keras picture Augmentation will zoom in and out to find out more about the image data shear range.

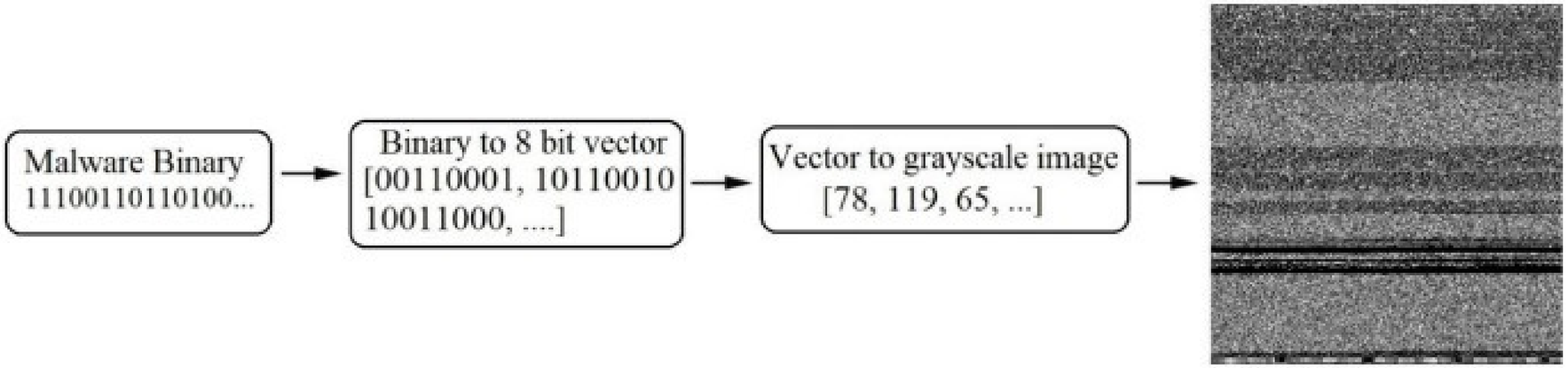

Fig-7. Conversion of PE file to grayscale

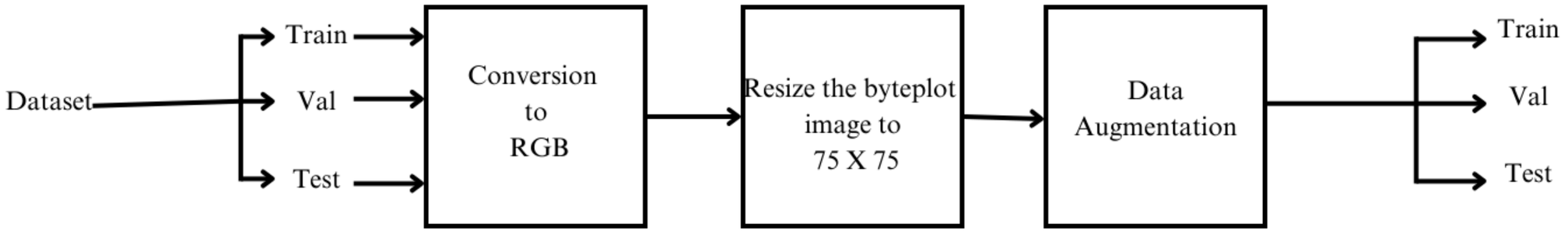

Fig-8. Image preprocessing

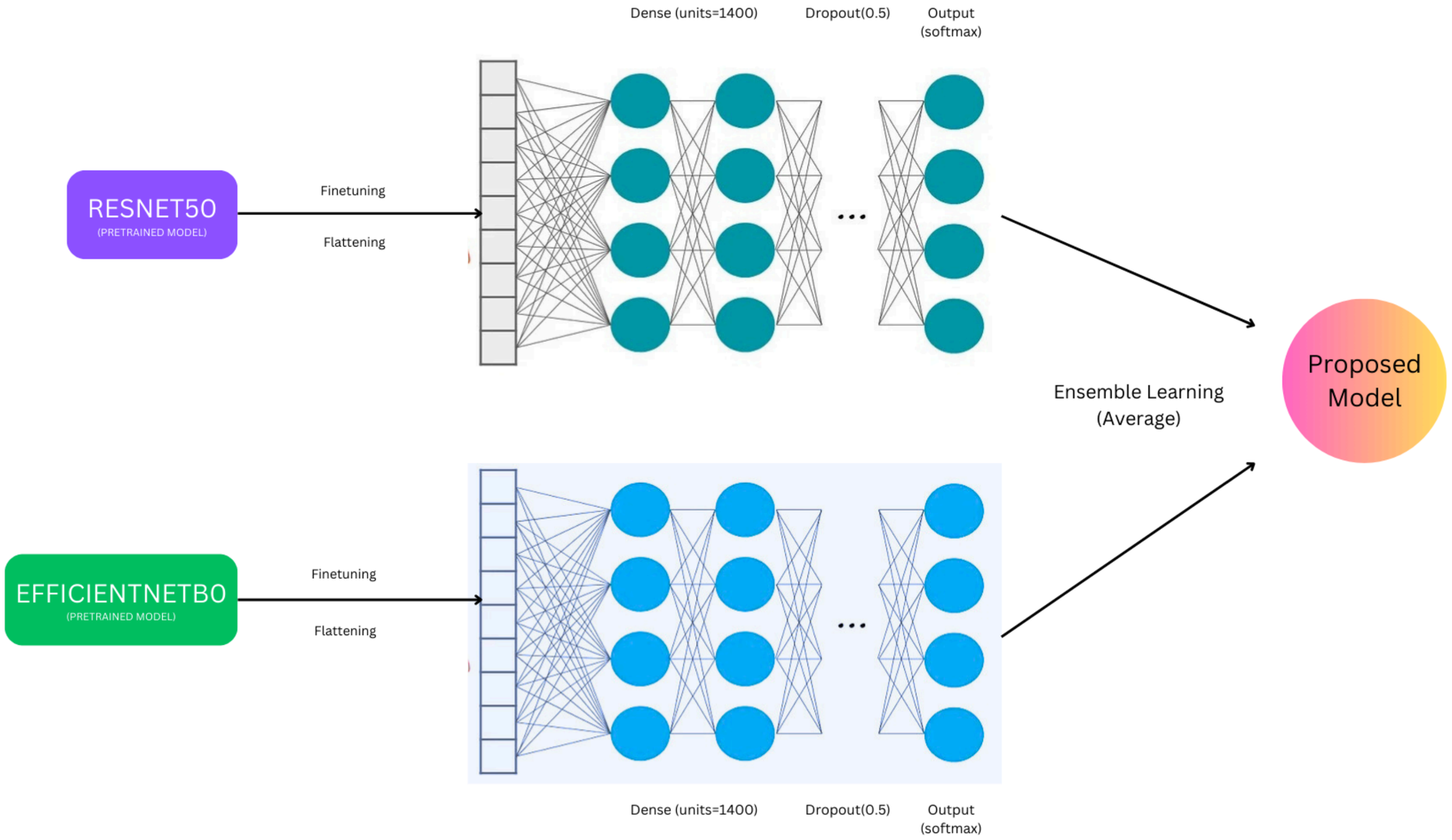

Fig.9. Overall Architecture of proposed model

Proposed Model Metrics

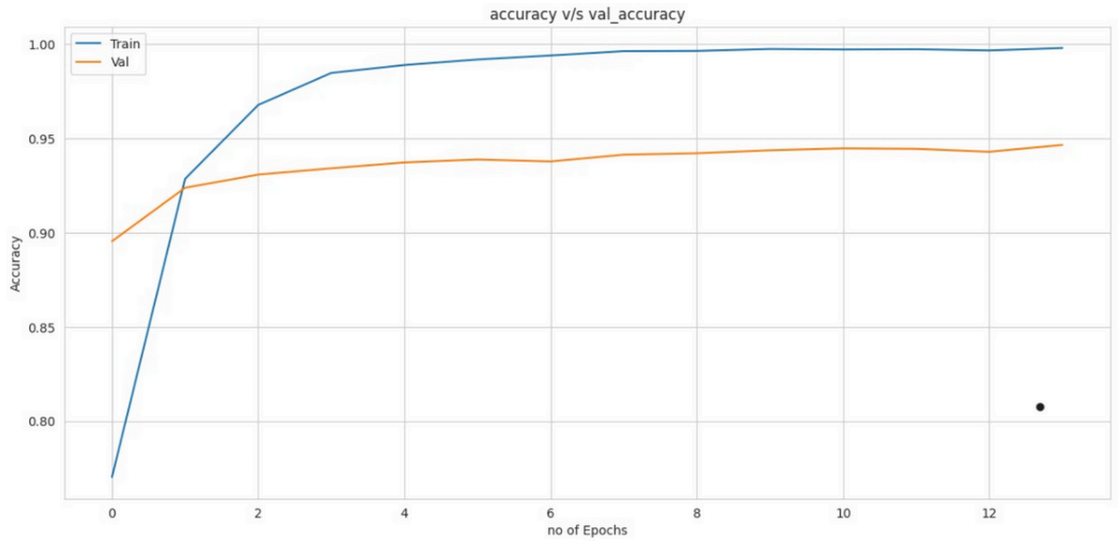

Fig.10 Classification Metrics for Proposed Dataset (Accuracy vs no. of epochs)

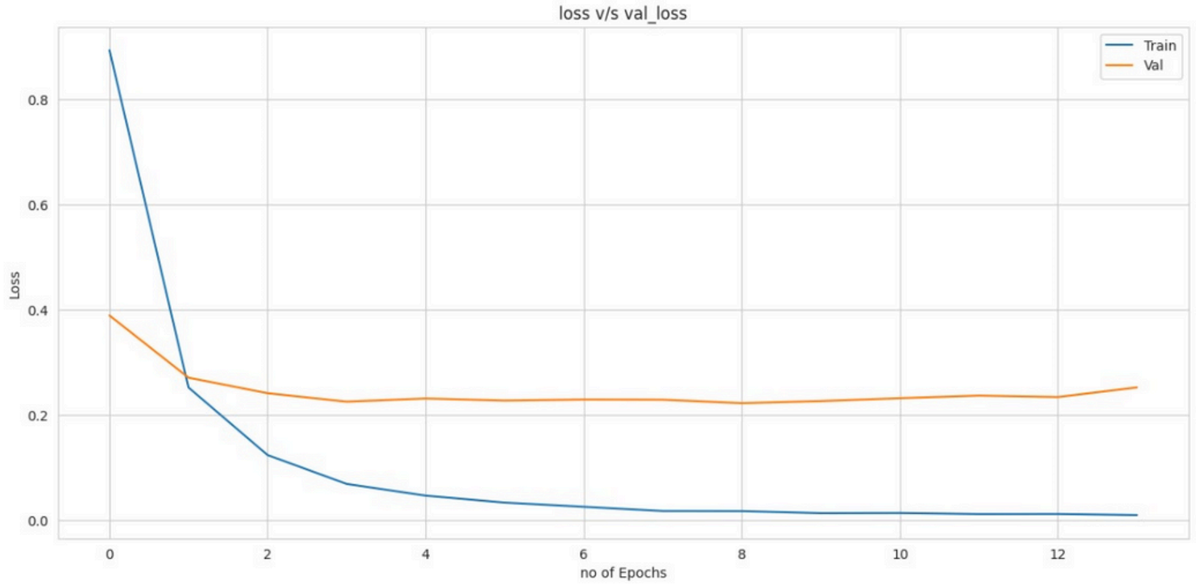

Fig.11 Classification Metrics for Proposed Dataset (loss vs no. of epochs)

Confusion Metrics for Proposed Model

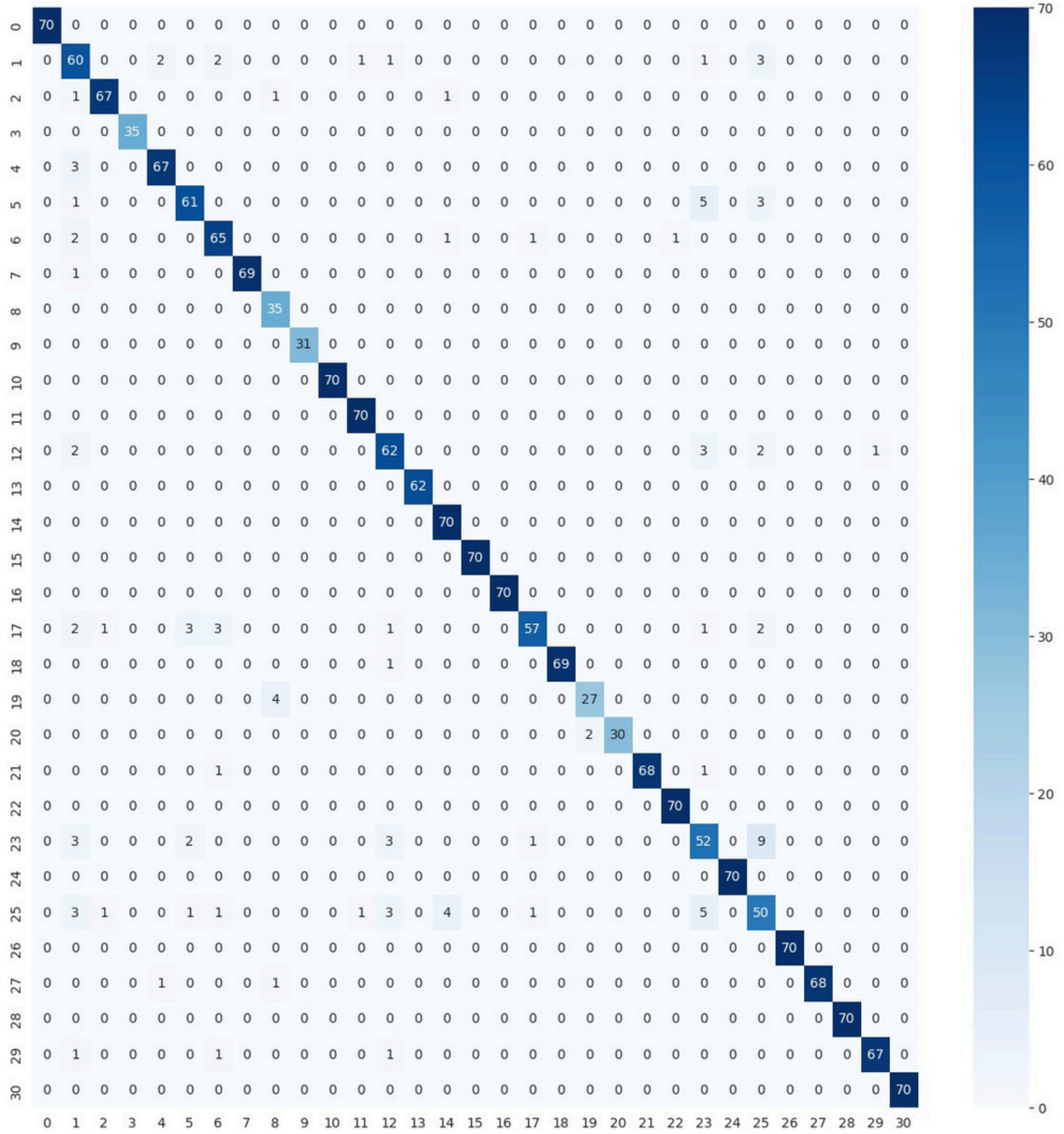

Fig.12 Confusion Metrics for Proposed Model

Result Analysis

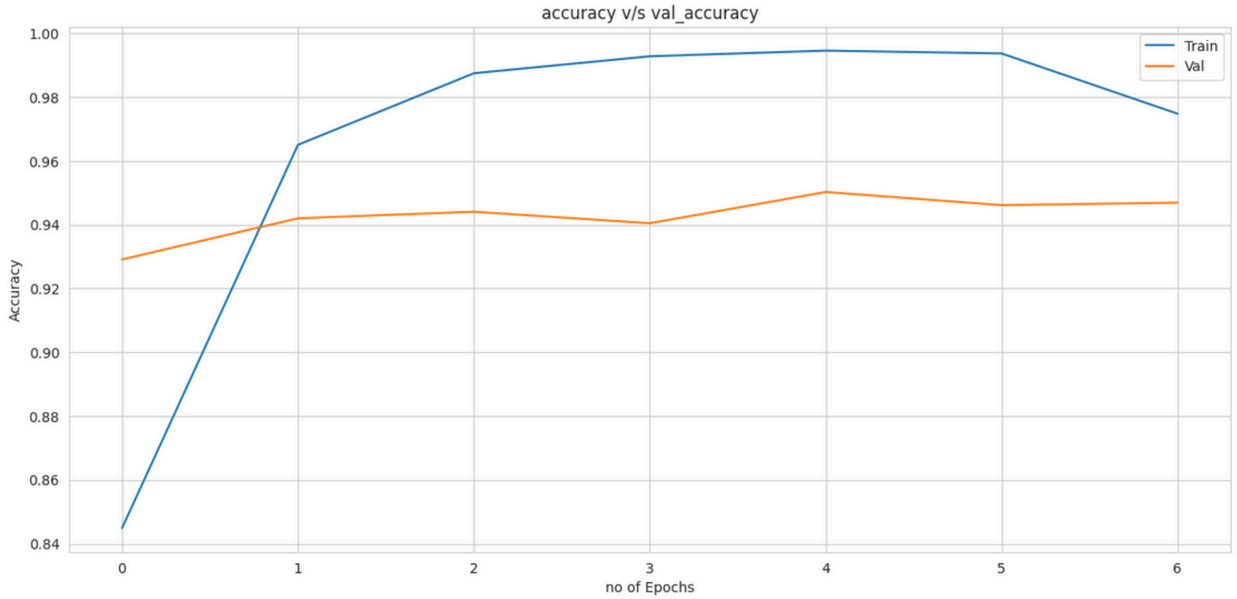

Fig.13 Accuracy graph for ResNet

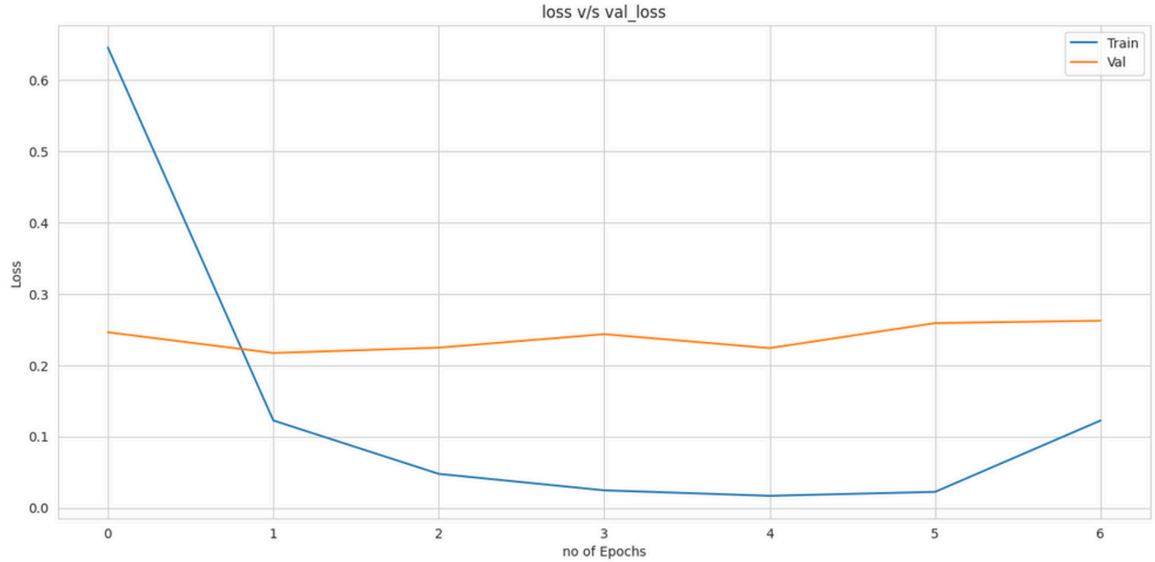

Fig.14 Loss graph for ResNet

Result Analysis

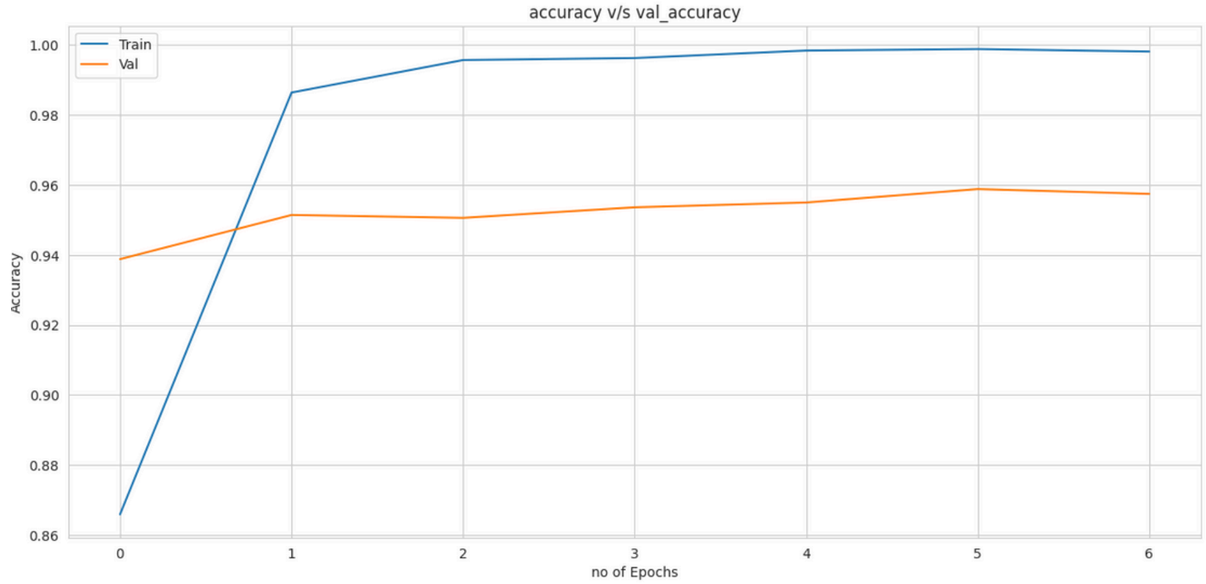

Fig.15 Accuracy graph for EfficientNet

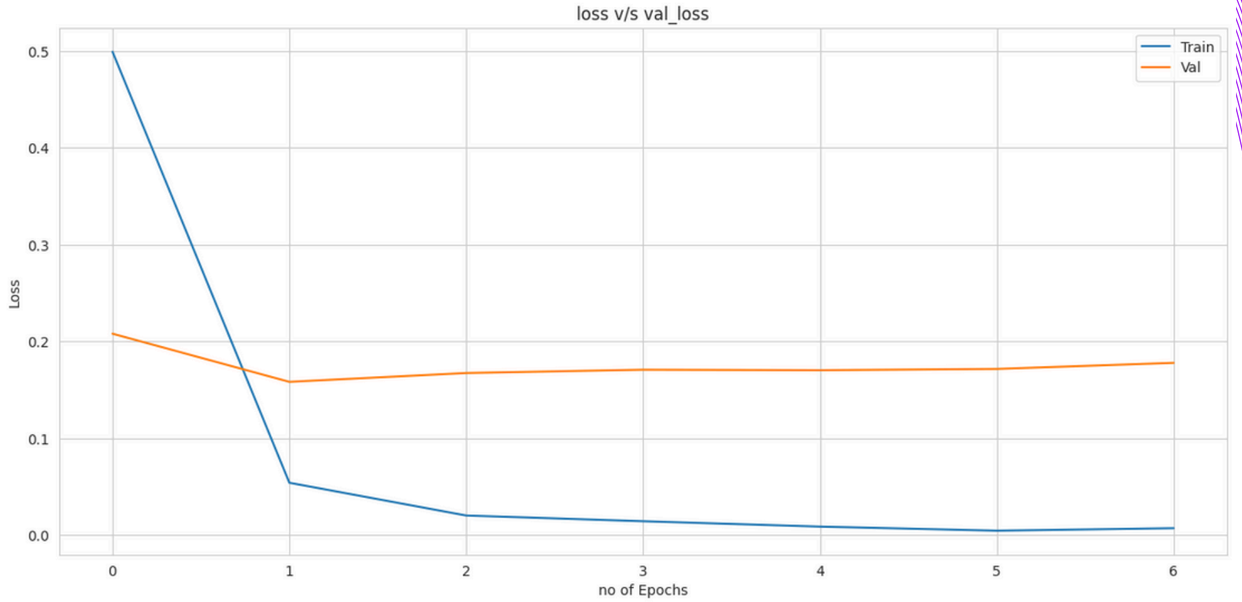

Fig.16 Loss graph for EfficientNet

Performance Evaluation Metrics

	ResNet	Efficient Net	VGG16	Proposed Model
Accuracy	0.95	0.95	0.93	0.97
Precision	0.95	0.95	0.92	0.96
F1 Score	0.95	0.95	0.93	0.96
Recall	0.95	0.95	0.93	0.96

Table 17. Classification Metrics for Proposed Dataset

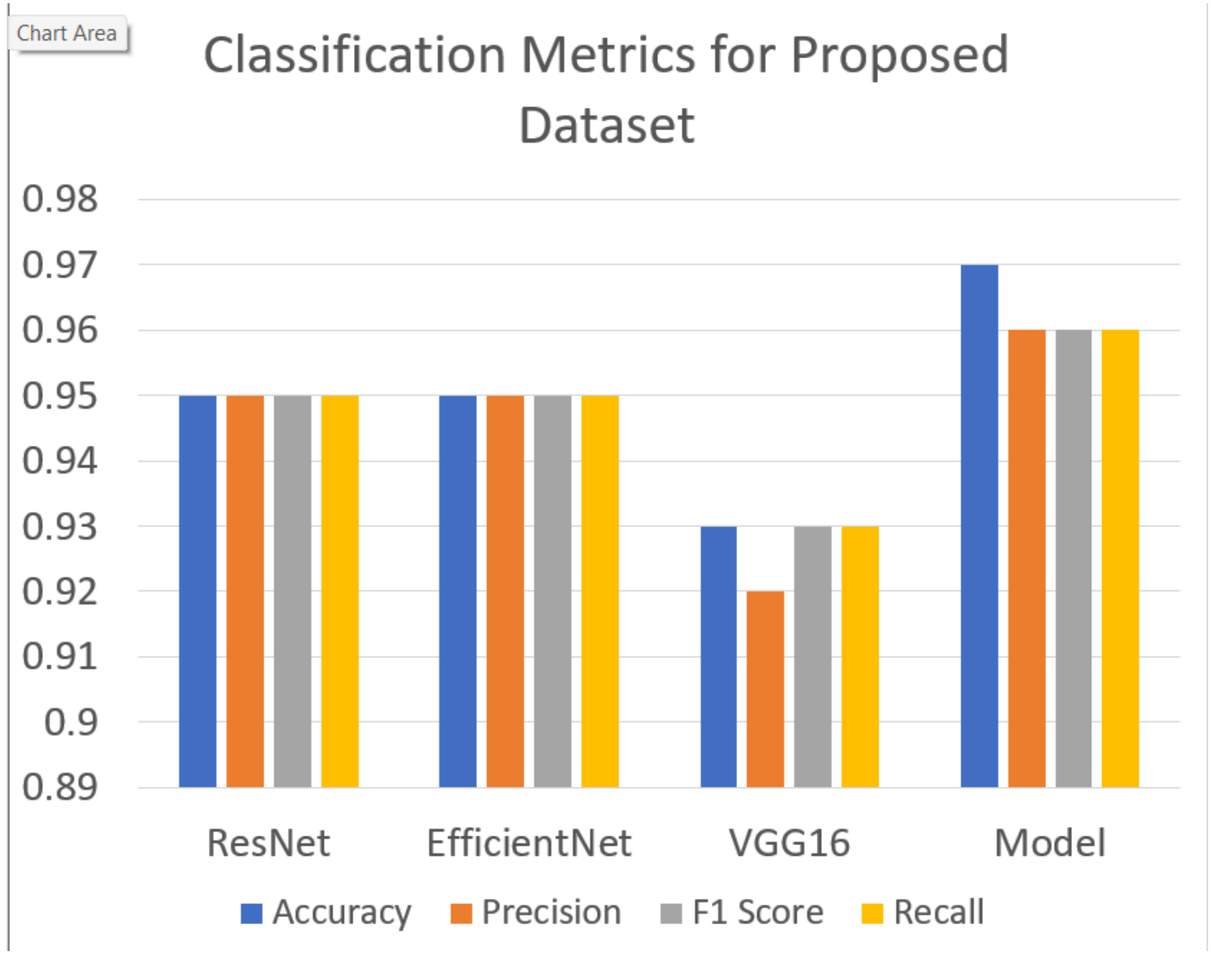

Fig.18 Classification Metrics for Proposed Dataset

Conclusion & Future Scope

Conclusion:

- The project is developed successfully with a novelty that a new semi balanced dataset is used by blending of two datasets.
- The proposed model detects and classify the malware using deep learning models (such as CNN) with an accuracy of up to 97% as compared to base model. But the model outperforms in terms of precision, F1 score and Recall value.

Future Work:

- **Use of Hyperparameter:** Our future scope is to use hyperparameters in ensemble learning to improve the accuracy. By optimizing these hyperparameters, the overall accuracy and robustness of the ensemble model for malware classification can be significantly improved.
- **Use of BIG2015 Microsoft Dataset:** The previous models are trained on BIG and classified dataset i.e BIG 2015 Microsoft dataset and Dumpware10 dataset which can be done using our ensembling model to enhance its accuracy and train it well.
- **Use averaging ensembling technique:** Enhance the model with weighted variance instead of averaging ensembling technique.

References

[1] Chaganti, Rajasekhar, Vinayakumar Ravi, and Tuan D. Pham. "Deep learning based cross architecture internet of things malware detection and classification." Computers & Security 120 (2022): 102779.
[2]Ren, Zhongru, et al. "End-to-end malware detection for android IoT devices using deep learning." Ad Hoc Networks 101 (2020): 102098.
[3]Ullah, Farhan, et al. "Cyber security threats detection in internet of things using deep learning approach." IEEE access 7 (2019): 124379-124389.

[4]Khan, Saddam Hussain, et al. "A new deep boosted CNN and ensemble learning based IoT malware detection." Computers & Security 133 (2023): 103385.
[5] Abusitta, Adel, et al. "Deep learning-enabled anomaly detection for IoT systems." Internet of Things 21 (2023): 100656.
[6] Vinayakumar, R., et al. "Robust intelligent malware detection using deep learning." IEEE access 7 (2019): 46717-46738.
[7] Raju, Anandharaju Durai, et al. "A survey on cross-architectural IoT malware threat hunting." IEEE Access 9 (2021): 91686-91709.
[8] Aslan, Ömer, and Abdullah Asim Yilmaz. "A new malware classification framework based on deep learning algorithms." Ieee Access 9 (2021): 87936-87951.
[9] Chaganti, Rajasekhar, Vinayakumar Ravi, and Tuan D. Pham. "A multi-view feature fusion approach for effective malware classification using Deep Learning." Journal of Information Security and Applications 72 (2023): 103402.
[10] Elayan, Omar N., and Ahmad M. Mustafa. "Android malware detection using deep learning." Procedia Computer Science 184 (2021): 847-852.