ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

Article Title: **CNN Classification based on the MobileNet for Malware Detection**

CNN Classification based on the MobileNet for Malware Detection

G. Kharmega Sundararaj[1,*], R. Sahila Devi[2]

[1]Associate Professor, Department of Computer Science and Engineering, Dr. T. Thimmaiah Institute of Technology, KGF, Karnataka, megaminindia@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Rohini College of Engineering and Technology, Palkulam, India. r.sahiladevi@gmail.com

ABSTRACT

The occurrence of harmful software, also known as malware is on the rise with certain types of malware becoming adept at camouflaging themselves within a system through sophisticated techniques. It is crucial to detect malware early on to prevent widespread damage to computer systems and the Internet. Numerous techniques for identifying malware have been created in recent times. Despite this, detecting malware remains a difficult task so this paper proposes the utilization of MobileNet-based CNN classification for malware detection. The initial dataset undergoes pre-processing to simplify the subsequent processes. Data preprocessing is a crucial step in data preparation where raw data undergoes various processing techniques to make it suitable for further processing. Data visualization involves transforming data into visual representations, such as charts or diagrams, to enhance comprehension and extract valuable insights for humans. These visualizations aid in understanding the data structure and detecting any anomalies present. MobileNet is specifically designed to reduce the parameter count, enhance training speed and provide accurate predictions. MobileNet is a convolutional neural network (CNN) design created specifically for the tasks of image classification and mobile vision applications. This makes it ideal for running on mobile devices or for implementing transfer learning techniques. To evaluate the model's performance, the confusion matrix is generated and this technology is well-suited for mobile devices, embedded systems and low-power computers that maintain a high accuracy without sacrificing computational efficiency. This work is implemented in python software.

Keywords: Malware, data pre-processing, data visualization, MobileNet based CNN classification, Confusion matrix.

1 Introduction

Malware, often known as malicious software which is a type of compiled binary file that disrupts networks or computer systems with the intent to encrypt, change or remove sensitive data, steal information or take over essential computer operations and some of the examples of malware are Ransomware, spyware, trojans and worms. There has been a significant surge in malware development recently, with an average of 588 cyber threats each minute [1]. Malware

exploitation infects a user's workstation and continue with some malicious activities such as collecting credentials, monitoring behavior, encrypting information and demanding a ransom. With 72.84% of the global smartphone market, the android Operating System (OS) is a market leader [2]. Furthermore, users download the applications from several markets, including the google play store and third-party marketplaces because the Android platform is open-source. Android's open nature and popularity have attracted malware attackers and in any application having a bad intention is named as harmful software (malware) [3]. Malware is designed to take control of a user's device, steal information and disrupt operating system operation. DOPS (Deep Ocean Protection System) is a basic EDR (Endpoint Detection and Response) system that incorporates the Endpoint Service Pack (ESP) and a malware detection mechanism based on images [4].

To improve performance, ESP requires better memory management, while Deep Ocean Malware Detector (DOMD) takes up a significant amount of disk and physical memory. In the future, ESP will require more micro service apps to expand existing services and add new components [4-5]. Deep learning approaches are increasingly being used to detect malware and network breaches using picture attributes and various neural network models and architectures are being developed and implemented. However, with numerous deep learning architectures and hyper parameters accessible, additional parameters is needed to identify the optimal solutions for cybersecurity [6]. IMCLNet is a lightweight model for malware classification with good feature extraction capability, a short training period and a small number of parameters. However, when these lightweight models are used directly to malware detection and classification activities, they do not generate highly accurate and efficient classification results, making it impossible to meet detection requirements [7-8]. The mobileNet based on malware detection method successfully detects IoT malware with high classification accuracy and minimal storage capacity, still it provides the method to demonstrate the effectiveness of opcode characteristics in malware detection and investigates aspects that impact model performance during feature fusion [9]. This unique strategy to detecting and classifying IoT malware utilizes deep Transfer Learning (TL) methodology, fine-tuning and ensembling strategies to boost performance without the need for training models [10]. In future, for further improvements a new Deep learning (DL) architecture using generative adversarial networks and transformers that enhances IoT malware detection and multi-classification performance by increasing unbalanced datasets is introduced [11-12]. Due to these demerits, the proposed system is implemented by introducing CNN classification based on MobileNet which is defined as the open-source platform in a google that provides a light weight in a training classifiers. Convolutional Neural Networks (CNNs) are popular deep learning algorithms for image classification where manual feature design is unnecessary as CNN provides a more accurate representation of the data [13]. Markov images and MobileNet are the methods that are used to detect malfunction, where the first process goes on with the extraction of opcode

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

sequences from malware's assembly code has been obtained. Secondly, by using the statistical information from opcode sequences the generation of markov images occurs [14]. A MobileNet consists of 28 layers, counting depth wise and point wise convolutions as separate layers. They have been tuned for efficiency and speed, while maintaining high accuracy in jobs like image recognition [15]. This paper proposes "Malware Detection on mobileNet using CNN classification" concerning the requirements on above papers. By concerning existing systems, the novel contribution introduced in this paper is:

- By using the convolutional neural network classification, the malware detection consume low resource to obtain better performance.
- Using CNN classification methods, hackers are kept away from the computer by using malware detection.
- The architecture obtaining the best performance by the Standard-CNN classification model, with a high accuracy. It also provides personal information from being the problem of leakage.

2 Proposed System Description

Due to the increasing number and complexity of malware threats, automated malware detection has become a hot topic in the field of network security. The field of malware analysis is rapidly growing and requires careful consideration due to the advancements in technology within social networks. CNN technologies have recently replaced traditional methods for identifying malware attacks. To combat this, a new system has been developed that utilizes CNN classification with MobileNet for more accurate malware detection.

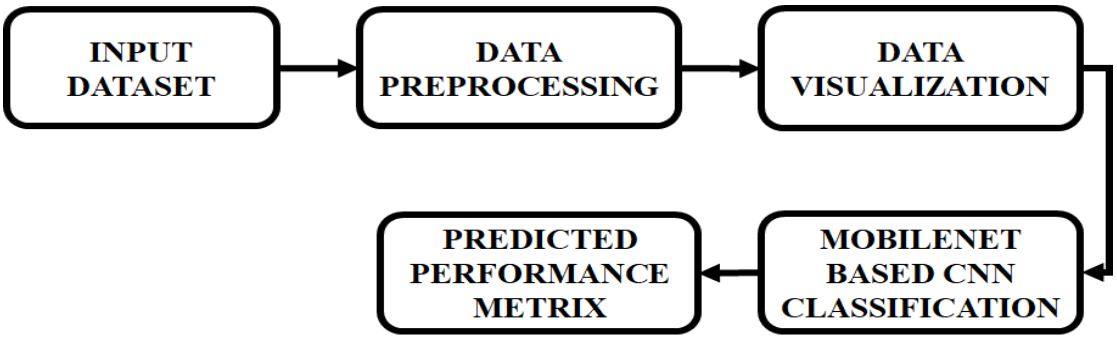

Figure 1: *Block Diagram of the Proposed System*

Figure 1 indicates the block diagram of the proposed system of CNN classification based mobileNet for the detection of malware attacks. The pre-processing method is used to improve the data quality so that analysing of data is more effective. Pre-processing method consists of two methods i.e., data preparing and data augmentation. Data preparation involves getting raw data ready for subsequent processing and analysis. Data augmentation is the technique of

transforming existing data into new generated data by making various adjustments to expand the dataset and balance the classes. Following data augmentation, the dataset goes through pre-processing before moving on to data visualization. Data visualization is the process of representing collected data using visualization tools to make it easier to interpret. Once data visualization is complete, the dataset is fed into MobileNet which is based on CNN classification. MobileNet classifies the dataset to improve the efficiency of predicting images, reducing the time required for recognition and comparison. This process also cuts down on the number of parameters, speeds up training and provides reliable forecasts. The datasets are then subjected to performance metrics that assess precision, specificity and overall performance and finally, the data is analyzed to achieve an accurate and efficient predicted output.

3 System Modeling

3.1 Data Pre–Processing

Data pre-processing is a fundamental step in transforming raw data into meaningful information. In general, raw data is incomplete, redundant or noisy. All of the concerns stated above will handled and used to generate machine learning models through data pre-processing. There are numerous data pre-processing tools and platforms available, including general-purpose computer languages and libraries such as Python, R and Pandas. Data pre-processing is necessary because good data is obviously more important than good models and the quality of the data is of fundamental importance. It is used to enhance privacy in information sharing and normal live detection does not require randomization. There are of two types of pre-processing techniques:

i) Data Preparation
ii) Data augmentation

i) Data Preparation

Data preparation is the process of making unprocessed information available for subsequent processing and analysis. The basic steps included in data preparation is collecting, cleaning and labelling the unprocessed data.

ii) Data Augmentation

The technique of creating new data from existing data in order to train new Machine Learning (ML) models. Data augmentation allows for the development of a large number of training samples to enhance the detector's robustness.

3.2 Data Visualization

Data visualization is the representation of gathered data and the system uses the visualization tools to transfer the data into easier patterns or methods. Data visualization is a vital phase in the data science process, allowing teams and individuals to more effectively communicate data

to colleagues and decision makers and this teams that administer reporting systems often use predetermined template views to monitor performance.

3.3 CNN Classification based on Mobilenet

Convolutional Neural Network (CNN) is a computer vision deep learning network that detects and categorizes data features and is impacted by the visual cortex's organization and activities. CNN has the ability to automatically find key features, but it also perform exceptionally well in tough settings such as complicated backgrounds and varying image resolutions and orientations. ResNet is based on the concept of Residual Blocks; typically, in a deep convolutional neural network, several layers are stacked; the network learns low/middle/high level features at the end of each layer. So, MobileNet is optimized for mobile and embedded devices, requiring only 16 MB of storage space. MobileNet is a computer vision model that is open-source and aimed for classifier training. It employs depthwise convolutions to dramatically minimize the amount of parameters compared to other networks, leading to a light-weight deep neural network.

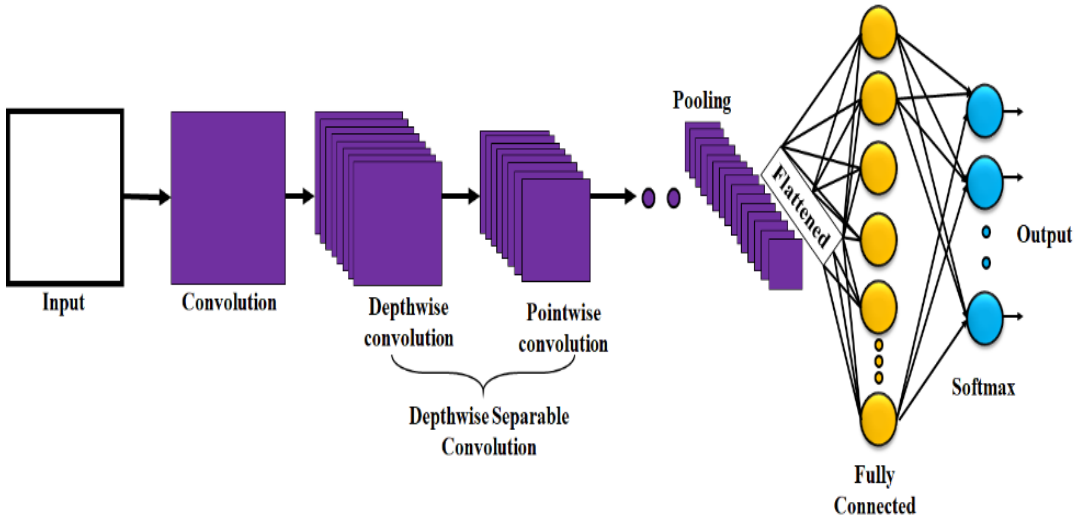

Figure 2: *Convolutional Architecture of MobileNet*

The enhancement of CNN's effectiveness in image prediction allows it to be competitive within mobile systems. The utilization of convolution methods significantly decreases comparison and recognition times, resulting in rapid and improved responses. This efficiency makes CNN an ideal choice for image recognition models. MobileNetV2 is a CNN architecture designed to perform effectively on mobile devices and it differs from conventional CNN architectures in that it connects bottleneck layers. Figure 2 and 3 represents detailed convolutional model and layered architecture of MOBILENET respectively.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

Article Title: CNN Classification based on the MobileNet for Malware Detection

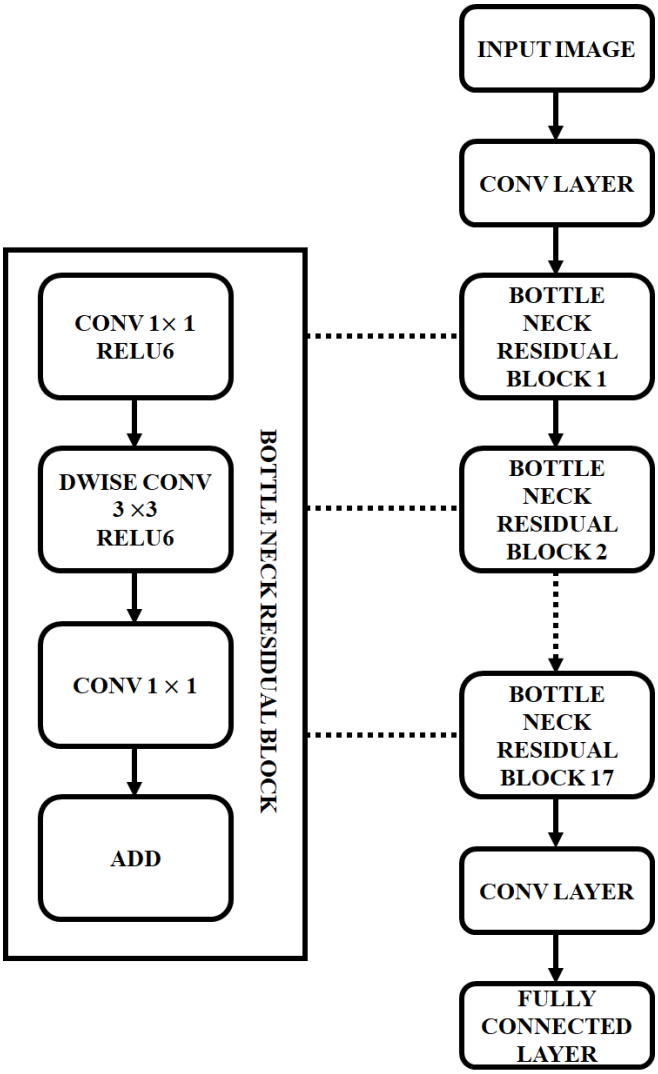

Figure 3: *Layered Architecture of Mobilenet*

4 Results and Discussion

In this paper, the detection of malicious attacks on MobileNet by CNN classification has been implemented. Python is a dynamically typed language known for its implementation technique and it is a high-level programming language that serves various general purposes.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

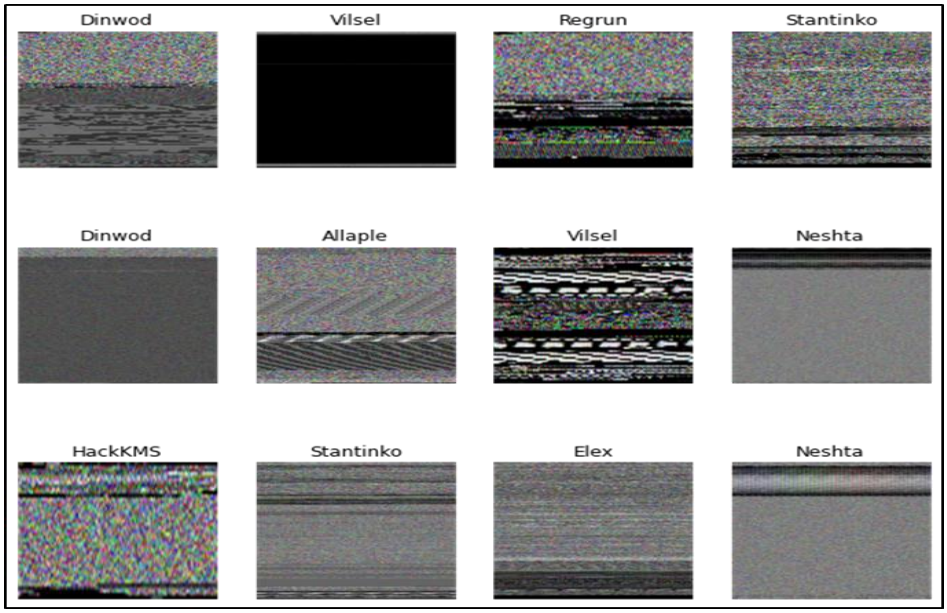

Figure 4: *Input Dataset*

Figure 4 represent the input dataset section that shows the result of several malware methods. The findings gathered from examining numerous malware samples to determine if the extracted byte sequences from the suggested technique offer valuable insights for manual analysis.

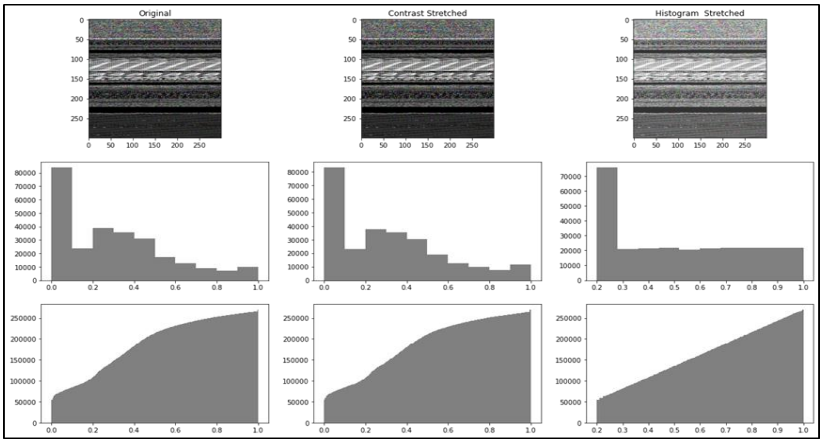

Figure 5: *Data Normalization*

Figure 5 represents the data normalization which gives the output of different data sections as cleaned and verified where improving the normalization process will enhance the accuracy of recognition.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

Article Title: CNN Classification based on the MobileNet for Malware Detection

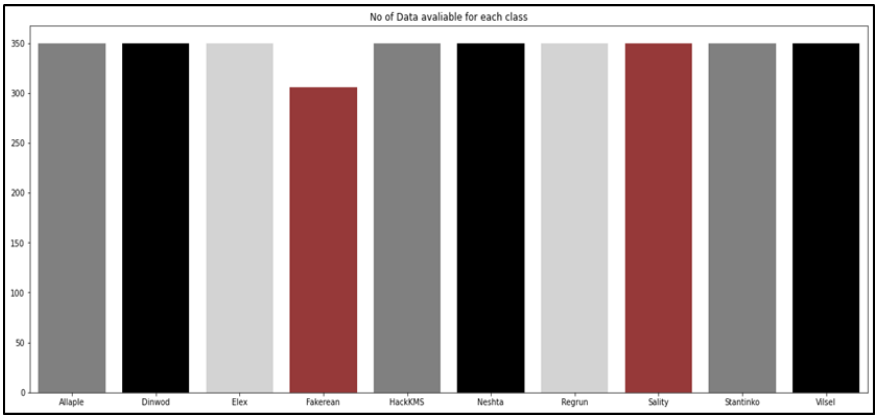

Figure 6: *Data Visualization*

The visualization in Figure 6 showcases the dataset representing different types of malware for classification. Data visualization is a powerful tool that enables individuals to visually interpret and comprehend complex datasets. By presenting information in a visual format, data visualization allows for easier interaction and understanding of data

```
Epoch 1/5
108/108 [==============================] - 222s 2s/step - loss: 0.4706 - accuracy: 0.8513 - val_loss: 0.1963 - val_accuracy: 0.
9354
Epoch 2/5
108/108 [==============================] - 208s 2s/step - loss: 0.1529 - accuracy: 0.9436 - val_loss: 0.1547 - val_accuracy: 0.
9543
Epoch 3/5
108/108 [==============================] - 209s 2s/step - loss: 0.0955 - accuracy: 0.9647 - val_loss: 0.1317 - val_accuracy: 0.
9579
Epoch 4/5
108/108 [==============================] - 223s 2s/step - loss: 0.0629 - accuracy: 0.9774 - val_loss: 0.1307 - val_accuracy: 0.
9572
Epoch 5/5
108/108 [==============================] - 208s 2s/step - loss: 0.0383 - accuracy: 0.9887 - val_loss: 0.1254 - val_accuracy: 0.
9586
```

Figure 7: *Accuracy Report for the Mobilenet*

Accuracy report on mobilenet is demonstrated on figure 7. In general, the proposed method has been validated for its classification performance. These findings confirm that the attention maps generated by the proposed method effectively describe the specific malware group.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 3(01), January 2024, pp. 39-51

Article Title: CNN Classification based on the MobileNet for Malware Detection

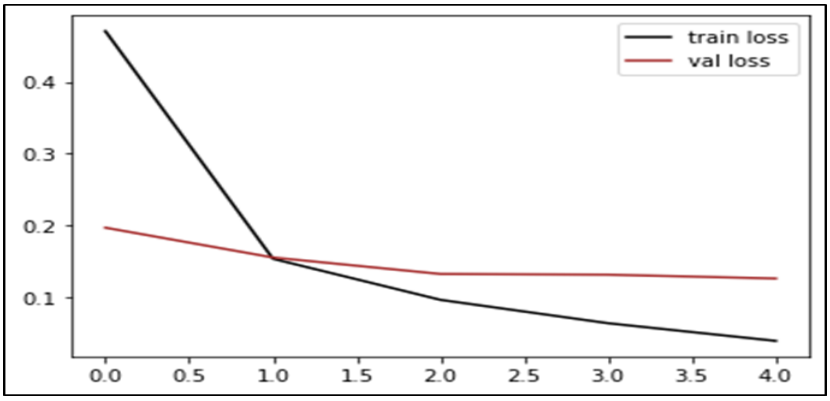

Figure 8: *Training Valid Loss of Mobilenet*

Figure 8 depicts the Training and Validation Loss of MobileNet.

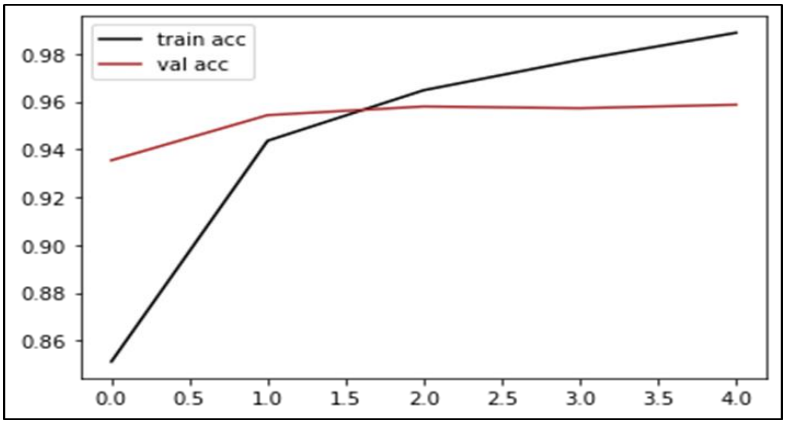

Figure 9: *Training and Valid Accuracy of Mobilenet*

The graph in Figure 9 illustrates the Training and Validation Accuracy of MobileNet.

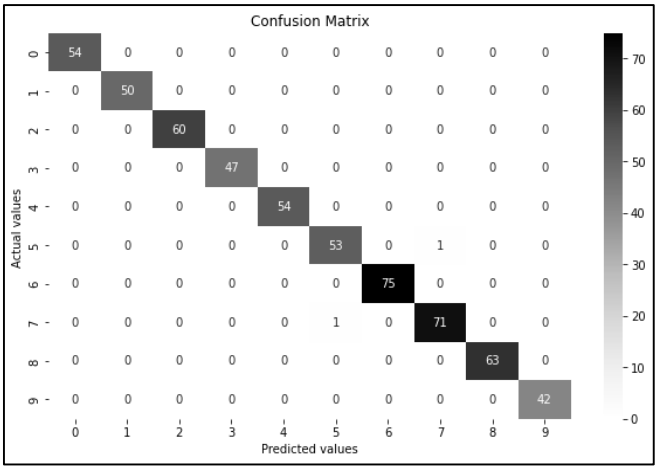

Figure 10: *Confusion Matrix of Mobilenet*

Figure 10 illustrates a confusion matrix of mobilenet. A confusion matrix is a chart that is utilized to evaluate the effectiveness of a classification algorithm.

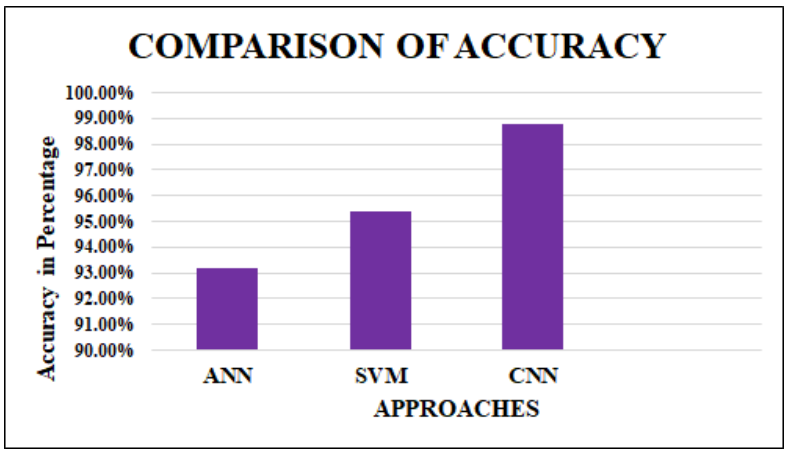

Figure 11: *Comparison of Accuracy*

Figure 11, a comparison is shown between the accuracy of Artificial Neural Network (ANN), Support Vector Machine (SVM), and Convolutional Neural Network (CNN) models. The accuracy of ANN is recorded at 93.2%, while SVM falls within the range of 95.4%. With the implementation of the proposed method, the accuracy of CNN significantly improves to 98.8%, surpassing the other models.

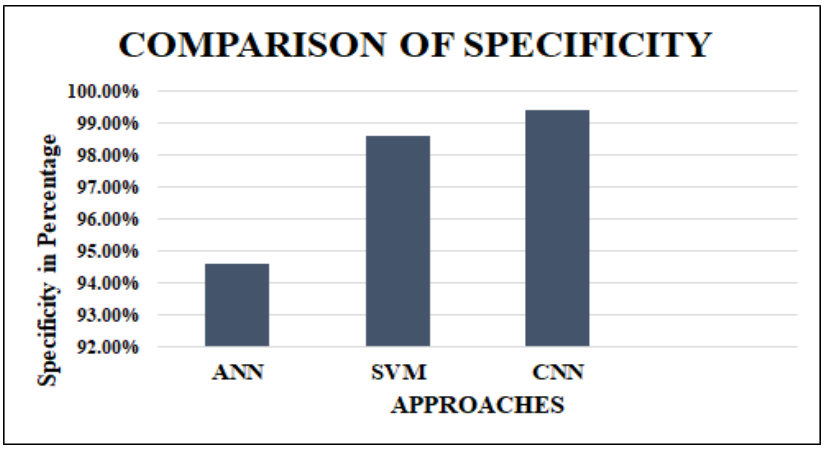

Figure 12: *comparison of specificity im mobilenet.*

In Figure 12, a visual representation is presented comparing the specificity levels of Artificial Neural Network (ANN), Support Vector Machine (SVM) and Convolutional Neural Network (CNN) models. The specificity of ANN is 94.06%, while SVM ranges around 96.7% through

the utilization of a suggested technique, the specificity of CNN experiences a substantial enhancement to 97.9%, surpassing the performance of the other models.

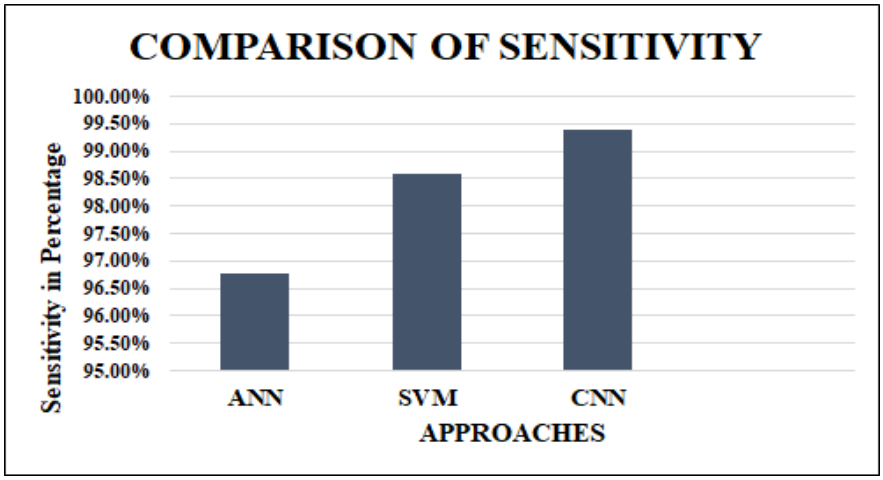

Figure 13: *Comparison of Sensitivity*

In Figure 13, a comparative analysis is depicted showing the sensitivity levels of MobileNet. The visual representation highlights the differences in sensitivity between Artificial Neural Network (ANN), Support Vector Machine (SVM) and Convolutional Neural Network (CNN) models. The sensitivity of ANN is measured at 96.78%, while SVM performs slightly better at 98.60%. However, by implementing a recommended technique, the specificity of CNN is significantly improved to 99.4%, surpassing the performance of both ANN and SVM models.

5 Conclusion

A proposed method using MobileNet-based CNN for malware detection is introduced in this study. The objective is to enhance the efficiency and accuracy in classifying and identifying different types of malware to combat the rising number of malicious codes. The performance and accuracy of the proposed method are assessed using a performance matrix. At last, the paper has effectively categorized and recognized various types of malware families utilizing MobileNet and this showcases the model's accuracy, sensitivity and specificity. This promising the application of MobileNet-based CNN for prompt malware classification is well performed. The utilization of MobileNet-based CNN for efficient malware classification has been successfully demonstrated. CNN demonstrates an impressive accuracy rate of 98.8%, with a specificity of 97.9% and a sensitivity of 99.4% concludes the performance surpasses that of both ANN and SVM algorithms.

References

1. Walid El-Shafai; Iman Almomani; Aala AlKhayer, Year: 2021, “Visualized Malware Multi-Classification Framework Using Fine-Tuned CNN-Based Transfer Learning Models”, Applied Sciences, Vol: 11, 6446.

2. Iman Almomani; Aala Alkhayer; Walid El-Shafai, Year: 2022, “An automated vision-based deep learning model for efficient detection of android malware attacks”, IEEE Access, Vol: 10, pp. 2700 – 2720.

3. Baraa Tareq Hammad; Norziana Jamil; Ismail Taha Ahmed; Zuhaira Muhammad Zain; Shakila Basheer, Year: 2022, “Robust Malware Family Classification Using Effective Features and Classifiers”, Applied Sciences, Vol: 12, 7877.

4. Tran Hoang Hai; Vu Van Thieu; Tran Thai Duong; Hong Hoa Nguyen; Eui-Nam Huh, Year: 2023, “A Proposed New Endpoint Detection and Response with Image-Based Malware Detection System”, in IEEE Access, Vol: 11, pp. 122859 – 122875.

5. Abdullah M. Alnajim; Shabana Habib; Muhammad Islam; Rana Albelaihi; Abdulatif Alabdulatif, Year: 2023, “Mitigating the Risks of Malware Attacks with Deep Learning Techniques”, *Electronics,* Vol: 12, no: 14, pp. 3166.

6. Omar A. Alzubi; Issa Qiqieh; Jafar A. Alzubi, Year: 2023, “Fusion of deep learning based cyberattack detection and classification model for intelligent systems”, Cluster Computing, Vol: 26, no: 2, pp. 1363 – 1374.

7. Binghui Zou; Chunjie Cao; Fangjian Tao; Longjuan Wang, Year: 2022, “IMCLNet: A lightweight deep neural network for Image-based Malware Classification”, Journal of Information Security and Applications, Vol: 70, pp. 103313.

8. Baoguo Yuan; Junfeng Wang; Peng Wu; Xianguo Qing, Year: 2022, “IoT Malware Classification Based on Lightweight Convolutional Neural Networks”, in IEEE Internet of Things Journal, Vol: 9, no: 5, pp. 3770 – 3783.

9. Changren Mai; Riqing Liao; Jing Ren; Yuanxiang Gong; Kaibo Zhang; Chiya Zhang, Year: 2023, “MobileNet-Based IoT Malware Detection with Opcode Features”, Journal of Communications and Information Networks, Vol: 8, no: 3, pp. 221 – 230.

10. Valerian Rey; Pedro Miguel Sánchez Sánchez; Alberto Huertas Celdrán; Gérôme Bovet, Year: 2022, “Federated learning for malware detection in IoT devices”, Computer Networks, Vol: 204, pp. 108693.

11. Ruitao Feng; Sen Chen, Xiaofei Xie; Guozhu Meng; Shang-Wei Lin; Yang Liu, Year: 2020, "A performance-sensitive malware detection system using deep learning on mobile devices", IEEE Transactions on Information Forensics and Security, Vol: 16, pp. 1563 – 1578.

12. Sharjeel Riaz; Shahzad Latif; Syed Muhammad Usman; Syed Sajid Ullah; Abeer D. Algarni; Amanullah Yasin; Aamir Anwar; Hela Elmannai; Saddam Hussain, Year: 2022, "Malware detection in internet of things (IoT) devices using deep learning", Sensors, Vol: 22, no: 23, pp. 9305.

13. Omar Habibi; Mohammed Chemmakha; Mohamed Lazaar, Year: 2023, "Performance evaluation of CNN and pre-trained models for malware classification", Arabian Journal for Science and Engineering, Vol: 48, no: 8, pp. 10355 – 10369.

14. Rajasekhar Chaganti; Vinayakumar Ravi; Tuan D. Pham, Year: 2022, "Deep learning based cross architecture internet of things malware detection and classification", Computers & Security, Vol: 120, pp. 102779.

15. Zhiyao Yang; Xu Yang; Heng Zhang; Haipeng Jia; Mingliang Zhou; Qin Mao; Cheng Ji; Xuekai Wei, Year: 2023, "An Android Malware Detection Method Using Multi-Feature and MobileNet", *Journal of Circuits, Systems and Computers*, Vol: 32, no: 17, pp. 2350299.