IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 2 (Mar. – Apr. 2024), PP 46-52
www.iosrjournals.org

Detecting Android Adware Using Transfer Learning With Computer Vision

Anika Tabassum[*1], Md. Asif Adnan Prince[2]
[1]*american International University Of Bangladesh, Dhaka 1229, Bangladesh.*
[2]*international University Of Business Agriculture And Technology-Iubat*

Abstract:
Adware, also known as advertising-supported malware, refers to unwanted software that displays advertisements. When adware infects a device, it can take root and compel the device to download specific adware variants. This behavior poses a significant threat to consumers, as attackers can exploit it to steal personal information. Despite its importance, there has been limited research on analyzing Android adware. In this study, we aim to utilize visualization and transfer learning techniques to detect Android adware. Specifically, we explore the use of pre-trained neural networks to identify adware within benign application package (APK) files. We evaluate the performance of several pre-trained models, including VGG16, ResNet 50, Inception v3, EfficientNet v2, and MobileNetv2. Our experiments, conducted using the CICMalDroid2020 dataset, demonstrate that the MobileNet v2 model achieves a maximum F1-score of 92% in detecting Android adware.

Keywords: *Android Adware, Computer Vision, Deep learning, Pre-trained model, Convolutional Neural Network (CNN), Transfer learning*

Date Of Submission: 16-03-2024 Date Of Acceptance: 26-03-2024

I. Introduction

People use their smartphones in both their personal and professional lives today thereby making them an essential aspect of life. There are an estimated 2.6 billion active smartphone users [1]. The rise in smartphone users has also led to an increase in malicious programs targeting mobile devices, that is, mobile malware. Malicious software (malware) is a program that has an intention of causing harm to the operating system kernel or some security sensitive application or data without the user's consent [1]. Criminals attempt to take advantage of flaws on other people's smartphones for their own gain. Additionally, over the past years' malware authors have become less recreational-driven and more profit-driven as they are actively searching for sensitive, personal, and enterprise information [2]. There has been an increase in the usage of handheld devices with the android platform having the larger market share, in 2018 the worldwide mobile application (app) downloads were approximated to be 194 billion [3]. With the growth in the adoption of technology, malware has become an increasing problem. Android is the most popular smartphone operating system in the world as of 2018 [4]. Since its release, sales of smartphones running on the android platform has grown strongly over the years [4]. Because of this popularity, android presents itself as an attractive attack platform for adversaries looking to maximize their impact on victims [5]. Applications like WeChat, TikTok, and mobile banking applications are used in our daily lives and continue to play an increasingly important role. Most of these applications have access to users' private information such as their location, debit/credit card, and contact information. Almost all applications access the users' private data, and although this provides users with better personalized services it may also result in information leakage of private data and economic loss. As cited by [6], Dogru et al. stated that android malicious applications keep on emerging continuously, and this security concern has gained increasing attention in both industry and academic fields. The android operating system has 72% mobile operating system market share for the period May 2019 to May 2020 [7]. By mobile operating system market share, android is the dominant player and with this, in combination with its liberal and open application marketplaces (compared to Apple's locked-down iOS application ecosystem), has meant that it has quickly become the mobile platform of choice for malware authors [8].

To address the plethora of malware and its associated security concerns, researchers are constantly developing and upgrading malware detection systems. Mobile malware detection is the process of classifying unknown mobile applications into benign and malicious [9]. There are different types of malicious software and one of these is called adware. Adware is a form of malware that downloads and displays unwanted advertisements, which are often offensive and always unsolicited [10]. Advertisements are used to promote or sell a product, an idea, or a service. The advent of the internet, and later the smartphone, has pushed

marketing strategies towards digitizing advertisements as it's the new normand the digital channel is rapidly growing with no signs of slowing down [11]. Shahzad et al. [12] states that the adware problem is growing continuously due to the profound monetary gains for adware developers, and it is largely agreed upon that user awareness of adware and its possible negative effects is still minimal. Avast, a global leader in digital security and privacy, reported that adware continues to be the most significant threat on android phones and tablets, with 45% of mobile threats being adware in the first five months of 2021 [13].

Because of the popular use, android devices present themselves as an attractive attack platform for numerous types of malwares with the following problems:

a) Proliferation of malware targeted at android mobile devices.
b) Malware authors using obfuscation techniques to make their malware difficult to detect using traditional static and dynamic methods of analysis.
c) Numerous zero-day malware that easily evades signature-based malware detection.
d) Highly specialized skills are required to analyse malware, and this involves huge volume of data for malware analysts to review which is time consuming and may lead to analysis fatigue.
e) The approach of using computer vision and transfer learning has not been utilized in analysing mobile android adware classification and detection.

The objectives of this research are:

a) Examine android adware.
b) Investigate transfer learning and computer vision techniques in android adware detection.
c) Evaluate the performance of pre-trained neural networks used in this research in detecting android adware.

Research Questions

To achieve the research objectives, an attempt to answer the following questions was made:

a) Can computer vision be applied in the detection of android adware?
b) Are the selected pre-trained deep neural network models effective in the detection of Android adware?
c) Which pre-trained deep neural network models used in
(b) will produce the best performance metric outcomes in the detection of android adware from benign apps?

Research Contributions

This research aims to contribute to the body of knowledge by firstly carrying out research work that leverages computer vision and transfer learning in to detecting android adware apps from benign android apps. Through knowledge obtained by reviewing various literature, previous work in this area has not utilized computer vision and transfer learning to detect android adware from benign apps. Secondly, performance evaluation was conducted on selected pre-trained convolutional neural networks to determine which of the pre-trained models performed the most effective and efficient in detecting android adware in this research.

Significance of Study

This research is important in that it will aid malware analysts in their efforts of analysing android adware from benign apps. In addition, it will reduce the time of carrying out malware analysis as it does not require expert knowledge in feature extraction due to the ability of deep learning models utilizing the automatic extraction of features on samples being tested. Though a lot of work has been done on android malware detection in general, very little focus has been put on the adware family [14], this research therefore expands on the work done in this area.

The scope of the research will be as follows:

a) The research will be focused on adware on the android platform.
b) The dataset used will focus solely on android adware and benign files that are free and publicly available.
c) The research will utilize selected pre-trained deep neural networks.

Data Collection and Pre-processing

The collected android APK files were obtained from the Canadian Institute of Cybersecurity at the University of New Brunswick from the dataset named CICMalDroid2020 [27] - [28].

The collected sample files were a total of three thousand and forty-eight (3,048) Adware and benign APK files. During the pre-processing some APK files were corrupted resulting in a lower number of files used in the experiments. The successfully processed files were broken down into, one thousand five hundred and fifteen (1515) android adware and one hundred and eight (108) benign APK files respectively.

Conversion of DEX File to Image

The APK files were processed to extract the classes.dex files from the APK and once the DEX files were extracted, we converted the DEX files into portable network graphics (PNG) format grayscale images. Example of the image files is shown in figure 2:

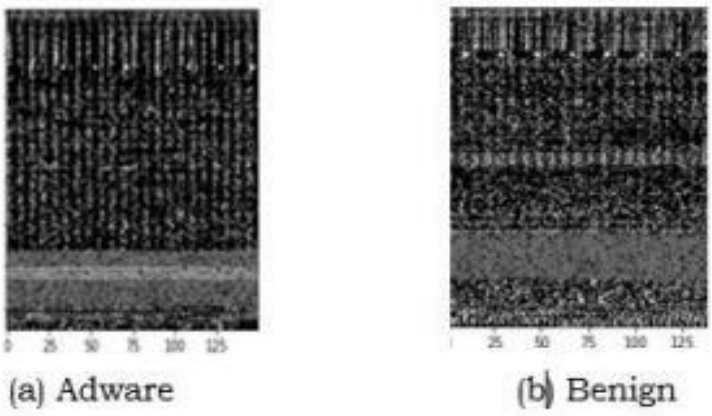

Figure 2. Sample Adware and Benign images

The images were split into training, validation and testing sets in the ratio of 70%, 20% and 10% respectively. Each input image file was resized to align with the default input image size of each pre-trained model that we used as indicated in the table 1.

Table 1. Image Input Size

SNO	PRE-TRAINED MODEL	IMAGE INPUT SIZE
1.	VGG16	224 * 224
2.	ResNet 50	224 * 224
3.	Inception V3	299 * 299
4.	EfficientNet v2	300 * 300
5.	MobileNet v2	224 * 224

Transfer Learning

The models used in the study were built using pre-trained models that are trained on a large-scale dataset called ImageNet [29]. It is a large database or dataset of over 14 million images. It was designed by academics for use in computer vision research. The models that we used were namely VGG16, ResNet50, Inception v3, EfficientNet v2 and MobileNet v2.

Evaluation

To evaluate the performance of the models four (40 performance measures of a binary machine learning (ML) -based classifiers were used. The following terms were used to quantify the results of each model using the confusion matrix:

True Positive (TP): an image is an ADWARE image and classifier marks it is as ADWARE
True Negative (TN): an image is a BENIGN image and classifier marks it is as BENIGN
False Positive (FP): an image is a BENIGN image and classifier marks it is as ADWARE
False Negative (FN): animage is an ADWARE image and classifier marks it is as BENIGN
Each of the performance measures used and their respective formula is defined below:
Accuracy: is the measure of all the correctly identified cases. It is most used when all the classes are equally important.

$$\text{Accuracy} = ((TP + TN) / (TP + FP + TN + FN)) \quad (1)$$

Precision: is the ratio of the probability that an app is classified as an adware app correctly.

$$\text{Precision} = TP/(TP + FP) \quad (2)$$

Recall: is the ratio of the total adware apps that are classified as adware.

$$\text{Recall} = TP/(TP + FN) \quad (3)$$

F-Measure or F1 score: It is a measure of a test's accuracy by considering both the precision and recall scores into a single measure of performance, where an F1-score is usually between 0.0 and 1.0 which closer to 1 is good while closer to 0.0 is poor performance.

F - Measure (F1 score) = 2* (Precision *Recall)/(Precision *Recall) (4)

Interpretation

With the establishment of the performance metrices the effectiveness of the models was derived from these values, with the highest percentage values indicating the best performing model in this research.

Development Environment

To perform the research work we used Jupyter Notebook development environment. For the dataset pre-processing, and Google Colaboratory or "Colab" for short was used to develop and train the models. Additionally, Anaconda Integrated Development Environment (IDE) was also used. This is a distribution of the Python and R programming languages for scientific computing, that aims to simplify package management and deployment. For the pre-processing, a system with the following specifications Intel (R) Core (TM) i3-6100U CPU @ 2.30GHz, 2304 MHZ, 2 Core(s), 4 Logical Processor(s) 8 GB RAM and 256 Solid State Disk Drive

For the development and testing of the model, Colab was used due to providing free access to computing resources and the following advantages:

It has pre-installed machine learning libraries such as Keras and TensorFlow.

It allows saving of work to the cloud.

Google Research provides their dedicated graphical processing units (GPUs) and tensor processing units (TPUs) for personal machine learning projects.

II. Results And Discussion

For each of the selected pre-trained CNN model stated in section 3.2 training was conducted and their performances compared with each trained model's performance output in this research.

The training and validation accuracy values began at high values due to the pre-trained model utilized the existing knowledge learnt previously on the ImageNet [29] database. The difference in the training and validation accuracies are an indication of the minimal model overfitting as the difference in values was not too wide. The training accuracy was derived from the training dataset and the validation accuracy shows how well the model performed on this data (the validation dataset) that the model had not previously seen.

The graphs below show the training and validation accuracy of each pre-trained model.

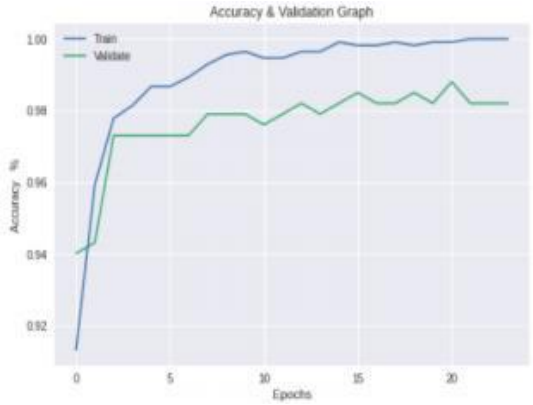

Figure 3. VGG16 Training & Validation Accuracy

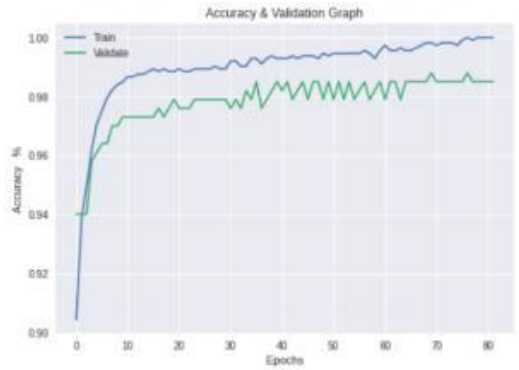

Figure 4. ResNet 50 Training & Validation Accuracy

Figure 5. Inception v3 Training & Validation Accuracy

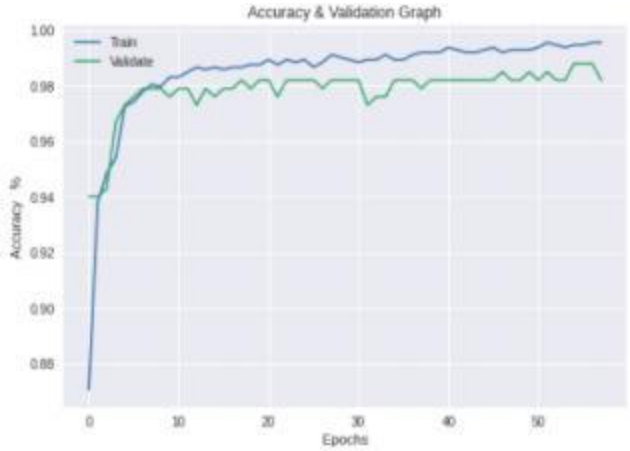

Figure 6. EfficientNet v2 Training & Validation Accuracy

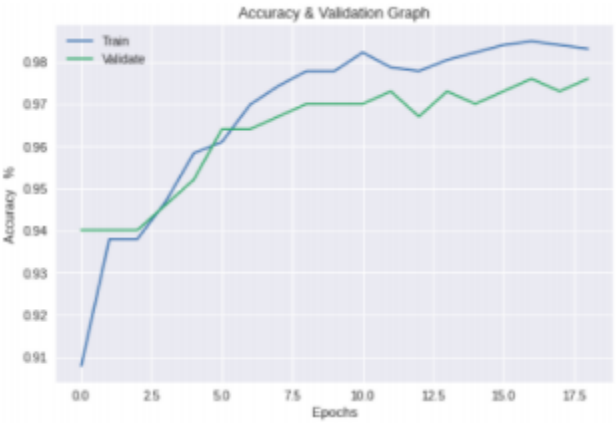

Figure 7. MobileNet v2 Training & Validation Accuracy

Table 2. Pre-Trained Model Performance

PRE-TRAINED MODEL	ACCURACY	PRECISION	RECALL	F1-SCORE	TRAINING DURATION (MINUTES)	EPOCHS
VGG 16	84%	91%	92%	91%	19	21
RESNET 50	81%	89%	91%	90%	45	82
INCEPTION v3	82%	90%	93%	91%	29	58
EFFICIENTNET v2	83%	90%	91%	90%	35	58
MOBILENET v2	83%	91%	94%	92%	26	19

From the experimental results obtained as shown table 2, we can see that the models produced model accuracy averaging 83% and an F1 -score average of 91%. On the F1 score metric, the MobileNet v2

had the highest value of 92% while the lowest F1 score was recorded by the ResNet 50 and EfficientNet v2 having a percentage of 90%. The training duration of the models varied amongst the models with the VGG16 model having recorded the least amount of training time of nineteen (19) minutes and the ResNet 50 pre-trained model took the longest by running for a duration of forty-five (45) minutes. The number of epochs also varied with the MobileNet v2 pre-trained model having the least number of epochs and ResNet 50 having the highest number of epochs.

Comparison with Prior Work

Bagui and Benson [14], used network traffic data available in the CICAndMal2017 dataset by Lashkari et al. [30] to analyse and classify adware families. They performed feature selection using information gain and classification was performed using traditional machine learning techniques, specifically J48 Decision Tree, Naïve Bayes and OneR. The results of the three classifiers, used as binary classifiers presented a highest average classification rate of 68% and highest average Attack Detection Rates (ADR) of 62.64% for the Adware families using the J48 Decision Tree classifier. This compared to the accuracy and F1-Score obtained in our research, which had a higher rate of 83% and 91% respectively. This shows that the use of computer vision in the research results obtained shows a significant improvement over previous work for classification of adware malware done in [14].

When a comparison is made with the proposed solution in the work done in [30], it was observed that the detection accuracy they had a higher accuracy and F1 score of 97.08% and 97.09% respectively compared to the accuracy and F1-score that was obtained in this research. Additionally, we compare the work done by Dobhal et al [23] in binary classification of Android Adware using various machine learning algorithms by illustrating results in the table 3.

Table 3. Comparison of the Proposed System with State-of-the-Art Approaches

Machine Learning Algorithm	F1 - Score	Accuracy
Logistic Regression (LR)	88%	71.12%
Linear Discriminant Analysis (LDA)	88%	79.28%
K-Nearest Neighbors (KNN)	83%	89%
Classification And Regression Trees (CART)	94%	91.72%
Naive Bayes (NB)	87%	77%
Average in proposed approach	91%	83%

As can been seen in table 3, apart from the Classification and Regression Trees (CART) algorithm, the F1 score the proposed approach outperforms the other algorithms used in [23].

In Suresh's dissertation [21] experiments were done with machine learning algorithms like Random Forests (RF), Support Vector Classifier (SVC), Ad boost and MLP respectively showing that using dynamic features alone for detecting android adware had an accuracy of about 76% however this was improved when experimented with combined features which resulted in an accuracy of about 84%. This does show that our obtained experimental results performed better when compared to the dynamic features approach used by [21]. However, the use of combined features approach in [21] shows a better performance than the proposed approach by 1% as the highest accuracy results obtained in our proposed approach was 83%.

III. Conclusions

Based on the outcome of the experimental work done in our research we confirmed that the use of visualization, image processing techniques and transfer learning when applied to binary classification and detection of android adware from android benign apps performs well as can be seen from the accuracy and F1 - Score metric values that we obtained. In comparison, each pre-trained deep neural network's performance results showed a small variance on all the performance metrics of accuracy, precision, recall and F1-score with the MobileNet v2 obtaining the highest F1 score. This leads us to conclude that pre-trained models that are created and adequately trained to solve a similar problem or task can be used to successfully detect android adware from benign apps. However, in contrast there was notable variation in the time taken to train the models with the VGG 16 and ResNet 50 taking the shortest time and taking the longest time respectively.

The study has shown that indeed transfer learning and computer vision sufficiently achieve the intended objectives and that the overall performance is adequate. We can therefore conclude that our experimental study was able to meet the set objectives with limitations noted and recommended as future works and areas of improvement.

IV. Recommendations

The work in this research aimed to establish the use of computer vision and transfer learning in android adware verses Android benign app binary detection. The study was able to show that this approach performs well and is comparable in performance and in some instances outperforms other methods. We therefore recommend for adoption of this approach in classifying and detecting android adware from benign apps.

References

[1] J. De Wit, "Dynamic Detection Of Mobile Malware Using Real-Life Data And Machine Learning", Masters Thesis, University Of Twente, 2018.

[2] K. Tam, A. Feizollah, N. B. Anuar, R. Salleh, And L. Cavallaro, "The Evolution Of Android Malware And Android Analysis Techniques", Acm Computing Surveys (Csur),Vol. 49,No. 4, P. 76, 2017.

[3] Https://Www.Statista.Com/Statistics/271644/Worldwide-Free-And-Paid-Mobile-App-Store-Downloads/ [Accessed 11th February 2022].

[4] Https://Www.Statista.Com/Statistics/266136/Global-Market-Share-Held-By-Smartphone-Operating-Systems/ [Accessed 11th February 2022].

[5] Sophos Ltd, Sophoslabs 2018 Malware Forecast. Oxford, Uk: Abingdon Science Park, 2017.

[6] X. Jiang, B. Mao, J. "Guan And X. Huang, "Android Malware Detection Using F"Ne-Grained Features", Scientific Programming, Vol. 2020, Pp. 1-2, 2020. Available: Https://Www.Hindawi.Com/Journals/Sp/2020/5190138/.

[7] [Accessed" 24 June 2020].

[8] "Mobile Operating System Market Share Worldwide | Statcounter Global Stats", Statcounter Global Stats, 2020. [Online]. Available:Https://Gs.Statcounter.Com/Os-Market-Sha Re/Mobile/Worldwide. [Accessed: 23- May- 2020].

[9] Sophos Ltd, Sophoslabs 2018 Malware Forecast. Oxford, Uk: Abingdon Science Park, 2017. A. Karnik, "Performance Of Tcp Congestion Control With Rate Feedback: Tcp/Abr And Rate Adaptive Tcp/Ip," M. Eng. Thesis, Indian Institute Of Science, Bangalore, India, Jan. 1999.

[10] N. Lu, D. Li, W. Shi, P. Vijayakumar, F. Picc"Alli And V. Chang, "An Efficient Combined Deep Neural Network Based Malware Detection Framewo"K In 5g Environment", Computer Networks, Vol. 189, P. 107932, 2021. Available: 10.1016/J.Comnet.2021.107932 [Accessed 25 June 2022].

[11] J. Gao, L. Li, P. Kong, T. F. Bissyandé And J. Klein, "Should You Consider Adware As Malware In Your Study?" 2019 Ieee 26th International Conference On Software Analysis, Evolution And Reengineering (Saner), 2019, Pp. 604-608, Doi: 10.1109/Saner.2019.8668010.