Library Progress International *Print version ISSN 0970 1052*
Vol.44, No.4, Jul-Dec 2024: P. 527-534 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

An Intelligent Malware Detection Model For Android Mobile Devices

[1]Akwukwuma Veronica N., ,[2]Egwali Annie O. ,[3]Asuquo Doris

Department of Computer Science. Faculty of Physical Sciences, University of BeninBenin City, Nigeria.nakwukwuma@uniben.eduannie.egwali@uniben.edudoris.asuquo@physci.uniben.edu

How to cite this article: Akwukwuma Veronica N., ,Egwali Annie O. ,Asuquo Doris (2024). An Intelligent Malware Detection Model For Android Mobile Devices. Library Progress International, 44(4), 527-534

Abstract

Android devices have experienced an immense popularity over the last few years. And this growth has exposed these devices to an increasing number of security threats. Despite the variety of peripheral protection mechanisms such as Bouncer, authentication and access control cannot provide integral protection against intrusions. Thus, the need for a more sophisticated security controls such as anomaly detection systems is necessary. Whilst much work has been devoted to mobile device intrusion detection systems, research on Android anomaly-based has been limited leaving several problems unsolved. Such as getting an error free detection technique or at least reducing the error to the barest minimum. Motivated by this fact, the researcher focused on anomaly technique of detecting Botnet on Android mobile devices. An open source malware database called Kaggle.com which is said to have a high malware detecting power was used. A cross-evaluation of three Machine Learning algorithms (i.e. Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbour (KNN. To check which of them detect with the highest accuracy and low False positive rate were considered. At the end the results of the three machine Learning models were then compared to know the best classifier for the model, and Random Forest came out as the best classifier with 99.99% accuracy and 0.013% false positive rate.

KEYWORD: Machine Learning, Botnet, Android, Anomaly, Malware, Accuracy and False Positive Rate (FPR)

Introduction

Mobile devices have become personal best friends to people across all ages (young and old); it has become an inseparable component in human lives. Also, mobile devices are fast replacing personal computers in terms of the ease of Internet usage by allowing users to have access to online services in real time and on-the-go. These devices have become popular in our lives since they offer almost the same functionality as personal computers. As part of utilising these mobile devices, certain sensitive data, such as contact lists, passwords, ATM card numbers, and bank verification numbers (BVN), are stored on them. Mobile devices face an everyday growing number of security threats (Vuleta, 2023). Recently, Vuleta (2023) of Legaljobs Lab identified 44 new mobile malware families to watch out for in the last quarter of 2023 (SMS trojans, iPhone malware, Android malware) with 23894 modifications. According to Kaspersky Lab reports of December 2020, their detection systems discovered an average of 360,000 new malicious files every day over the past 12 months, of which most are botnets. This discovery represented an upward increase of 5.2% from 346,000 in 2018. Mobile malware is specifically written to attack mobile devices such as iPhones, Android tablets, and smartwatches. The hackers rely on the exploits of these mobile operating systems and mobile phone technology. Mobile malware has become a challenge to the security industry as attacks increase in frequency and strength (Vuleta, 2023; Kaspersky, 2020). It is designed to spread from one unprotected device to another. The malware authors used many techniques to evade detection, such as a) requisition for unwanted hardware, b) encryption, c) code obfuscation technique, d) download or update attack, in which a benign application updates itself or another application now with a malicious payload, which is very tough to detect (Barriga & Yoo (2017).

Hackers used many types of malware to attack mobile devices. There are different types of malware that attack mobile devices; some of them are ransomware, Trojans, phishing, etc. And since most mobile devices are connected to the internet most of the time, the malware can easily be transferred from any infected system to another. This connection is where Botnet comes in. A botnet is a network of devices infected by malware that runs automatically once a user installs it on a device in the network. The botnet itself is not malware; it is a network of connected devices that has been infected by malware. These malware gains complete access to all the devices in the network and their contents and starts communicating with and receiving instructions from one or more command and control servers controlled by a cybercriminal called a botmaster. Phishing attacks often come in the form of email or SMS and convince the victim to disclose account credentials or to install malware. The attacker masquerades as a reputable entity or person and distributes malicious links or attachments that can extract login credentials or account information from victims. Phishing does not only steal identity and information from victims; it also steals data. No matter the type of malware that has infected the network, they are all intruders, and this study is to find a way of detecting the intruder—malware. Intrusion detection is software that identifies an intruder in a system and reports such an intruder. A malware intrusion is any activity that is designed to compromise the security of a device (Mesevage, 2019). This intrusion can also be an attempt by hackers to gain access to a system. In our world today, data is what drives most business decisions; the more data one has, the more information one can access. One of the activities of cybercriminals is stealing users' data and making users exceed their data limit. When it comes to security, finding the outliers is only the first step; determining the outliers as a security threat is another; and understanding the root cause of the outlier is the key to a real solution. The goal of botnet detection is to identify behaviours that are unusual within data that is seemingly comparable.

The mobile platform considered here is the Android mobile platform; this is because it has the highest market shares of 85.9% as of June 2021 (Stat Counter, 2021) and 70.1% as of the last quarter of 2023 (Sherif, 2024). Another reason that makes Android devices popular is that Android-based smartphone users can get free applications from the Android Application Market (Play Store), but these applications, if not certified by legitimate organisations, may contain malware that can steal users' private information (Stat Counter, 2021). To repel these cybercriminals, there is a need for intelligent anomaly detection techniques for effective security of our devices (Android mobile). However, because of the popularity of Android devices, hackers have turned their attention to it, where it is possible to obtain enough of their preferred data, especially when security issues are taken less seriously by the users of those devices. So, keeping the system safe from intrusion is one of the most essential parts of system security. If an attacker invades a system, it will lead to significant loss of data. Therefore, it has become necessary to provide various technical solutions to detect malware and protect the content of this mobile device. For many people, mobile devices are their main and only device to store sensitive information about themselves, and this kind of data is what the attackers are interested in. According to Kaspersky, (2022). Solution detected 400,000 new modifications of mines. Kaspersky asserted that the number of malicious files detected every day increases by 5% in 2021. Kaspersky (2022) opined that the number of attacks detected by their laboratory in February 2022 was 16,897, which grew to 48,597 as of March 2022.

Going by the statistics of Vuleta (2023) of Legal Jobs Labs, one can imagine the number of victims in this era of cashless policy. As cybercrime becomes more threatening and rampant, and as a mobile device user who has seen the problem caused by these cybercriminals. There should be a way to encourage other mobile users to be aware of their mobile devices. Research efforts in this area have been intensified, producing various methods of detecting and defending the devices against cybercrimes. To date, ML-based detection methods have proven to be quite effective, though not without their limitations, such as timely detection, detection error, real-time monitoring, adaptability to new threats, and so on. Detecting with high false alarms and not so good accuracy rates are some of the issues still to be solved. Different ML methods have different strengths and weaknesses, as seen in the role they play in cyber securities. It has become necessary to provide various technical solutions to protect the contents of mobile devices from malware (software) or botnets (hardware). It is very common these days to receive a call from a criminal telling you that they are calling from your bank, and the criminal will give you a few details about your account, then turn to ask you for the one they cannot access easily so as to clear your account. Keeping your system safe from malware attacks is one of the most important parts of system security. If the system is penetrated by a malicious attacker, it can lead to massive loss of data.

The driving force for this research is to detect and stop the activities of cyber criminals by using a model that will detect malware in Android devices with high accuracy and little or no false alarm that is false negative or false positive. False positives occur when a system identifies a legitimate or benign file as malware. While false negative is uncaught malware that has successfully evaded detection. According to Kubovic (2019), false positives (FP) can be much more costly than a malware infection. What is meant here is that when a protection solution incorrectly labels a clean item as malicious. This may lead to the item being quarantined, blocked, or even deleted; therefore, it is important to deal with these errors. According to Kaspersky (2022), there is a dangerous rise of a notorious Android botnet known as Emotet. And this type

of botnet specialises in extracting different kinds of data, especially financial data, from infected devices. Their research showed that the number of victims shot up from 2,843 in February 2022 to 9.086 in March 2022. Also, the number of attacks detected by Kaspersky solutions has also grown accordingly, from 16,897 in February 2022 to 48,597 in March 2022. Since most Android phones are connected most of the time, it is easy for criminals to trick vulnerable Android users into giving out their financial data, and this helps the criminals log into their account to steal their money. Kim et al. (2013) proposed a hybrid intrusion detection tool that used decision trees for the classification of malicious and benign applications. They designed an automatic feature extraction tool written with Java scripts that can extract two features: permission and method API. To evaluate their framework, they collected 893 normal applications from the Android market and 110 malicious applications from the Internet site and had a detection accuracy rate of 82.7%. Canfora et al. (2015) proposed an Android malware detection method that is different from other methods; their method was based on selecting the longest sequences of system calls for the malware detection rather than considering the individual system call invocation by the Android application. They used the SVM machine learning algorithms for malware detection and achieved a detection rate of 97%. Kurniawan et al. (2015) used Logger, a default application that is inbuilt in Android, to extract the sum of Internet traffic, percentage of battery used, and battery temperature for every minute. This information is collected as a set of features and fed into WEKA, an open source learning library for testing and training with Naive Bayes, J48 decision trees, and Random Forest algorithms. The author concluded that Random Forest has a high accuracy of 85.6% with these features and proposes other features that can be combined with existing systems to improve the accuracy. The authors only mentioned that the false positive and false negative rates were high; their focus was on accuracy rate, so they compared four different algorithms and decided that random forest produced the highest accuracy rate of the four.

Abah et al. (2015) also designed a model called HOSBAD; this is a machine learning approach for the detection of malware on Android platforms. The system monitors and extracts features from the applications while in execution and uses them to perform in-device detection using a trained K-Nearest Neighbour classifier. Their results showed performance in the detection rate of the classifier with an accuracy rate of 93.75%, an error rate of over 6%, and a claim of a low false positive rate, which was not specified. KNN could only work on small data sets and cannot guarantee realistic assessment. As there is the possibility of some malware evading detection, the error rate of 6% is high.

Meng. & Spanoudakis (2016). In their model, MBotCS (a mobile botnet detection system based on machine learning) made use of five machine learning algorithms: Naive Bayes, KNN, SVM, Decision Tree, and Neural Network. Their average accuracy rate was 87% and their error rate was 13%. All the ML tools used in their work only work well in small datasets, apart from their individual weaknesses. Tariq and Baig (2017) used a decision tree to detect botnets in software-defined networks. The model came out with 97% accuracy. The problem here is the weakness of the decision tree being that any small change in data can lead to a large change in the structure of the optimal decision tree, thereby making it unstable. Miller (2018) used Support Vector Machine (SVM) to detect botnets in Android mobile, and their model recorded a high rate of accuracy of 86%. With a high false alarm rate of 23%. SVM has issues when the number of features for each data point exceeds the number of training set samples; it underperforms. Rasheed et. al. (2019). In their botnet detection in Android, they used the WEKA tool technique and got 85% accuracy. The WEKA tool can only handle a few megabytes, and this is the era of big data. Whenever a set is bigger than a few megabytes, an out of memory error occurs. And this can cause false alarms. Gyunka and Barda (2020) used the idea of Bezerra et al. (2019), whose work was based on OC-SVM, but instead of SVM, they decided to use the KNN classification approach and developed a normality model that is based on the One-Class K-Nearest Neighbour (OC-kNN) machine learning approach for anomaly detection of Android malware. The OC-kNN was trained using WEKA 3.8.2 Machine Learning Suite through a semi-supervised procedure that contained mostly benign and a very few outlier Android application samples. The OC-kNN had 88.57% true performance accuracy for normal instances, while 71.9% was recorded as true performance accuracy for outliers (unknown) instances. The false alarm rates for both normal and outlier's instances were recorded as 28.1% and 11.5%. The model recorded a high false positive rate because the KNN classifier works better on small datasets and is sensitive to the scale of data and irrelevant features.

Yerima (2021) used the deep learning method to obtain a 97.6% accuracy rate as against 97.1%. Hijawi et al. (2021) used four popular ML classifiers: Random Forest, Multi-Layer Perceptron Neural Network, Naive Bayes, and. Each group of features undergoes training and testing processes using the four ML classifiers. After comparing the results and performing feature importance analysis, it was shown that the Random Forest classifier obtains the best results based on all sets of features at 98%. Motylinski et al. (2022) use IoT combined with a machine learning approach for detection of botnet attacks; they have an accuracy rate of 95%. Alissa et al. (2022) used decision trees, the XgBoost model, and logistic regression models, trained, tested, and evaluated on the dataset. In addition to model accuracy, F1-score, recall, and precision are also considered. Based on all experiments, it is concluded that the decision tree outperformed with 94%

test accuracy. Negera et al. (2022), in their model, made use of IoT and machine learning. They reported a high detection rate of 92%.

Alani (2022) used deep learning classification models; their model was evaluated using different performance indicators (PI). The indicators are accuracy and error rate. The model had 90% accuracy rate and 10% error rate. Mudassir et al. (2022) used multilayer deep learning approaches for detection of botnet attacks against industrial IoT systems. Their work recorded a 91% accuracy rate. Almuhaideb and Alynanbaawi (2023) use artificial intelligence to detect Android botnets. Using algorithms like support vector machine (SVM), decision tree, and multi-layer perceptron, the data set is trained and tested. After the training and testing, the decision tree model has good accuracy and performance of 92%. Sri et al. (2023). In their study, three popular classification machine learning algorithms—Naive Bayes, Decision Tree, and Neural Network—as well as the ensemble methods known to strengthen said classifiers are evaluated for enhanced results related to botnet detection. This evaluation is conducted with the CTU-13 public dataset, measuring the training time and accuracy scores of each classifier. They concluded that the decision tree has the highest accuracy rate of 92%, and it also has a very low value of false positive and false negative.

Hoang and Nguyen (2018) worked on a botnet detection model based on machine learning using domain name service query data and evaluated its effectiveness using four popular machine learning techniques (K-Nearest Neighbour, Random Forest, Decision Tree, and Naive Bayes). Their results show that machine learning algorithms can be used effectively in botnet detection. The model achieved an overall classification accuracy of over 90.80% and a false positive rate of 9.80%. They suggested that in the future, larger datasets can be used to analyse the effects of the domain name features on the detection accuracy, as well as new features to improve the detection accuracy of the proposed model.

Botnet needs to be detected with high accuracy rate and very little or no error rate, either False positive of False Negative. According to Bohutska (2021), the percentage of false positive that can be considered low should be lower than 27.8% and anything higher is considered as high. Gyunka and Barda (2020) in their work stated that their False positive rate was 28.1% which is higher than 27.8% as stated by Bohutska (2021). Also Hu et al (2018) suggested that there was limitation in their work and that the limitation was detecting of hidden anomalies. The point here is that, if anomaly that has not been detected is present, that means there is false positive or false negative. Garcia-Font et al., (2016) also suggested among others that a future study should be made to reduce the false positive rate to the barest minimum and to improve the detection performance. Hoang and Nguyen (2018), also suggested among others that future analysis be made with new features (classifiers) to improve the detection accuracy of the model. Their results showed performance in the detection rate of the classifier with high accuracy rate of 90.8%, error rate of over 9.8%, Their result showed a better performance in terms of error rate as compared to Bohutska (2021) benchmark, hence the use of their work as the existing system. The proposed system used anomaly based method of detection together KNN, RF and SVM. Then the results for KNN, SVM and RF will be compared and the classifier with the highest accuracy and lowest false positive will be choosen as the best classifier among the three.

The question now is:

1. To what extent can SVM, RF KNN detect Mobile Bot with higher accuracy?
2. How can SVM, RF and KNN detect Bot with lower FPR as compared to the bench mark of 27.8% as stated by Bohutska (2021)?
3. Which of the classifiers work best for the proposed model?

There have been significant research efforts on the problem of Android malware detection. Some researchers used one classifier, others two; others used as many as ten. Also note that each of these classifiers has their strengths and weaknesses. The use of classifiers and the number depends on the preference of the researchers. Below are some of the researchers that work on Android malware detection and botnet detection using various detection techniques and different datasets.

Methodology

Basic steps of the new system design make use of object-orientated analysis and design methodology. The design stage is the process of defining the problem in terms of real-world objects with which the system must interact and software objects used to explore various solution alternatives.

Description of the system framework

I. The Requirement Stage: Data Collection

Android malware dataset is collected from Kaggle.com data repository.

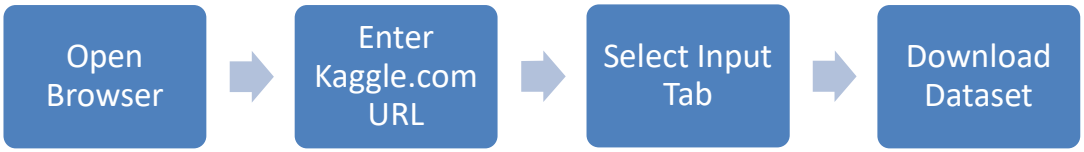

Fig 1: Dataset collected from Kaggle.com data repository

II. The Design Stage: Data Pre-processing

Android malware dataset is pre-processed to eliminate redundant features using Principal Component Analysis (PCA). The data is also partitioned into training and test set.

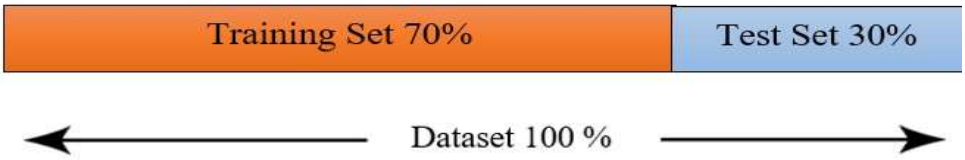

Fig 2: Partition of Train and Test set

III. Construction Stage: Model Training

The training set is used in the training of the 3 machine learning models –Support Vector Machine (SVM), Random Forest (RF), K-Nearest Neighbour (KNN).

```
from sklearn.model_selection import train_test_split

x_train, x_test, y_train, y_test = train_test_split(X, y, test_size = 0.3)
```

Figure 3: Data Partitioning

System Framework

The proposed model for an intelligent detection model for effective security of android mobile devices is presented below;

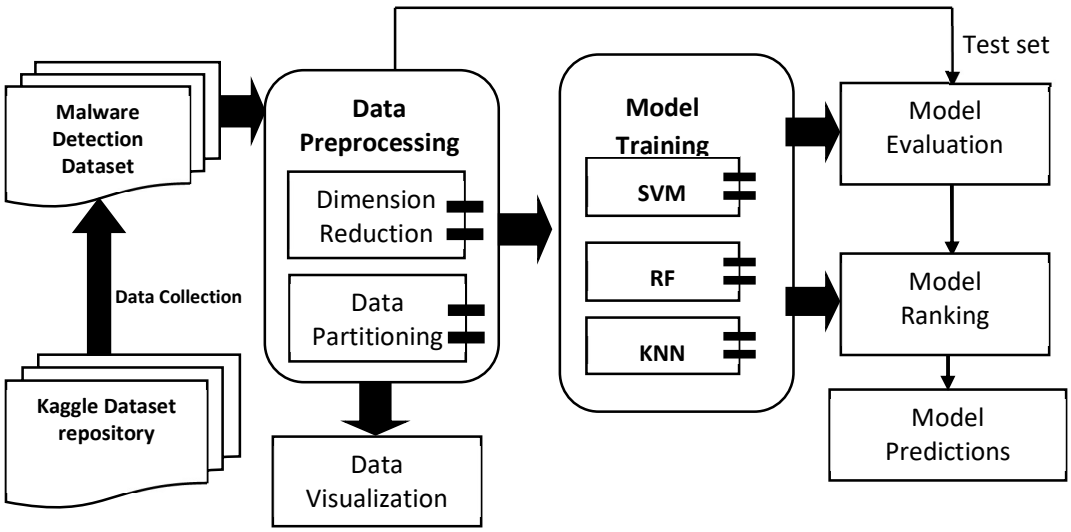

Figure 3. The Proposed Model

The graphical representation of the models performance is presented in Figure 3

IV. **Model Testing and Evaluation:**

The trained models in Step 3 are evaluated using the test set based on accuracy.

V. **Model Predictions and Ranking:**

The trained models in **Step 3** are ranked based on their performance (Accuracy). Model with the highest accuracy is selected as the **best** performing model.

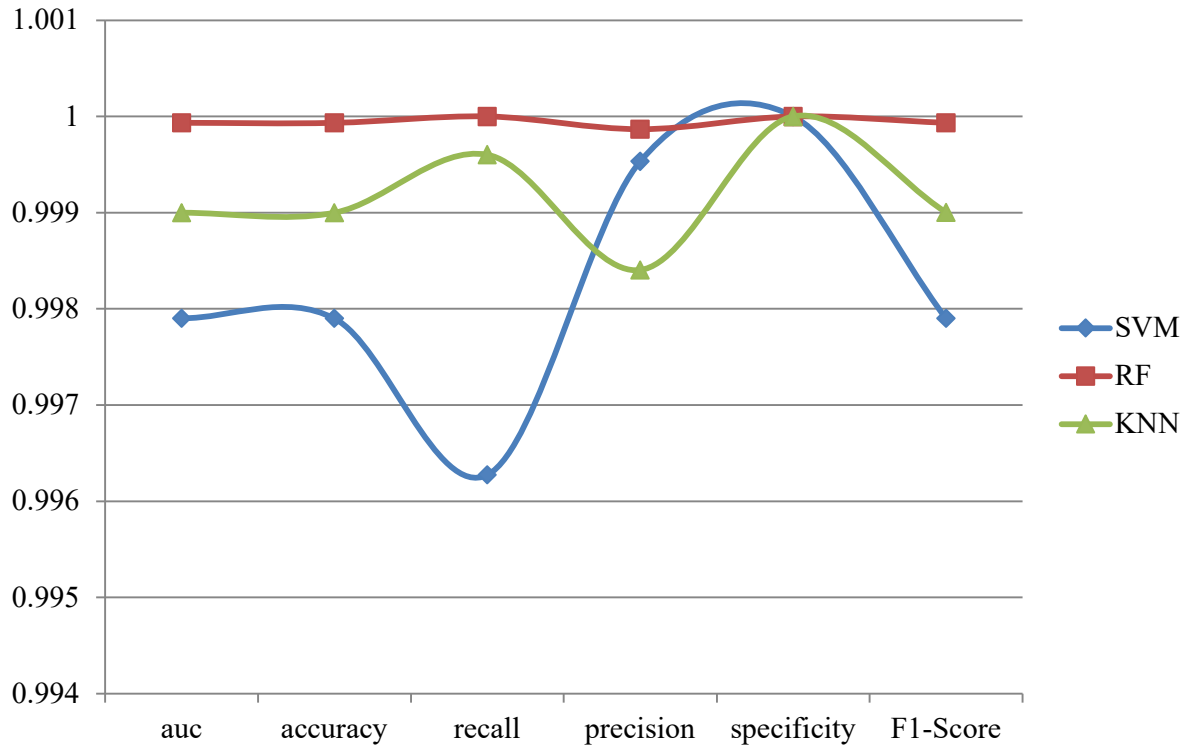

Figure 4: Models Performance

The performance of the SVM, RF and KNN, used in this work is presented in Table 1

Table 1 Models Performance

Model	AUC	Accuracy	Recall	Precision	Specificity	F1-Score
SVM	0.997903	0.9979	0.996274	0.999533	1	0.9979
RF	0.999933	0.999933	1	0.999867	1	0.999933
KNN	0.998999	0.999	0.999601	0.998405	1	0.999002

From Figure 3 and Tables 1 and 2, it is observed that RF (Random Forest) outperforms SVM, and KNN, to emerge as the best model for effective Android Botnet detection.

9.0 Summary of Result

The table below presents the performance comparison between the three classifiers and the comparison is carried out on the basis of the accuracy and f1-score and False Positive Rate (FPR).

Table 2: Comparing the Models

Models	Accuracy	F1-Score	FPR
KNN	99.9601	99.9002	0.167
RF	99.9933	99.9933	0.013
SVM	99.79	99.79	0.046

10.0 Answers to research question:

1. **To what extent of Accuracy can SVM, RF KNN detect Mobile Bot?**
   Support Vector Machine (SVM) detect accuracy with 99.79%, Random Forest (RF) with 99.99% and K- Nearest Neighbour (KNN) with 99.96%
2. **How can SVM, RF and KNN detect Bot with lower FPR as compared to the bench mark of 27.8% as stated by Bohutska (2021)**

From the result obtained, SVM detect malware in Android with FPR of 0.046, KNN with 0.167 while RF detect with the smallest FPR of 0.013. So the proposed Model detected malware with very small FPR which is way smaller than the benchmark.

3. To determine which of the classifiers work best for the proposed model?

Random Forest is the Classifier that work best for the model, with the highest accuracy and lowest FPR

11.0 CONCLUSION

An intelligent anomaly detection model for effective security of Android mobile devices was proposed. Kaggle.com dataset was used, and 3 machine learning models—Support Vector Machine (SVM), Random Forest (RF), and K-Nearest Neighbour (KNN)—were used. The model achieved improved performance by reducing false alarm rates and increasing accuracy. In comparison, it was observed that Random Forest (RF) outperforms SVM and KNN, making it the best classifier for the proposed model.

REFERENCES

- Abah, J., Waziri, O.V., Abdullahi, M.B., Arthur, U.M., and Adewale, O. S (2015). A Machine Learning Approach To Anomaly-Based Detection On Android Platforms. International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.6, November 2015 DOI : 10.5121/ijnsa.2015.7602 15
- Alani, M.M (2022). BotStop : Packet-based efficient and explainable IoT botnet detection using machine learning**.** Computer Communications Volume 193, 1 September 2022, Pages 53-62. https://doi.org/10.1016/j.comcom.2022.06.039Get rights and content
- Alissa, K., Alyas, T., Zafar, K., Abbas,Q., Tabassum,N., and Sakib, S. (2022). Botnet Attack Detection in IoT Using Machine Learning. Computational Intelligence and Neuroscience Volume 2022, Article ID 4515642, 14 pages https://doi.org/10.1155/2022/4515642
- Almuhaideb, A.M. and Alynanbaawi , D.Y. (2023). Applications of Artificial Intelligence to Detect Android Botnets: International Conference on Machine Learning and Data Engineering. Digital Object Identifier 10.1109/ACCESS.2022.3187094
- Barriga, J.J. and Yoo, S.G. (2017). Malware detection and Evasion with Machine Learning Techniques: A survey. International Journal of Applied Engieering Research 12(18).7207 - 7214.
- Bezerra, V. H., Da-Costa, V.G.T., Barbon-Junior, S., Miani, R. S. and Zarpelão, B.B.(2019). "IoTDS: A One-Class Classification Approach to Detect Botnets in Internet of Things Devices," Sensors (Switzerland), vol. 19, no. 14, pp. 1–26, 2019.
- Bohutska,J.(2021).How to tell good performance from bad. https://towardsdatascience.com/anomalydetection/
- Canfora, G., Medvet, E., Mercaldo, F. and Visaggio, C.A.(2015). "Detecting Android Malware Using Sequences of System Calls," in Proc. 3rd Int. Work.Softw. Dev. Lifecycle Mob., pp. 13–20, 2015.
- Garcia-Font,V., Garigues, C., & Pous, H. R. (2016). *A comparative Study of Anomaly Detection Technique for Smart city wireless sensor network*.
- Gyunka,B. A. and Barda,S. I.(2020). Anomaly Detection Of Android Malware Using One-Class K-Nearest Neighbours (Oc-Knn). Nigerian Journal of Technology (NIJOTECH)/Vol. 39, No. 2, April 2020, pp. 542 - 552 http://dx.doi.org/10.4314/njt.v39i2.25
- Hijawi, W., Alqatawna, J., Al-Zoubi,A.M., Hassonah, M.A., Faris, H.(2021). Android botnet detection using machine learning models based on a comprehensive static analysis approach. Journal of Information Security and Applications Volume 58, May 2021, 102735
- Hoang, X.D. and Nguyen, Q. C. (2018). Botnet Detection Based On Machine Learning Techniques Using DNS Query Data. *Future Internet*, 10 (43); doi:10.3390/fi10050043 www.mdpi.com/journal/futureinternet
- Hu, X.L.,Zhang, L.C and Wang,Z X.(2018). An adaptive Smart Phone anomaly detection An Introduction.bmc.Https://www..bmc.com/blog/machine learning.
- Kaspersky (2022). The number of new malicious files detected daily. From : https://www.kaspersky.com/about/press-releases/2020_the-number-of-new-malicious-files-detected-every-day-increases-by-52-to-360000-in-2020 December 15, 2020 retrieved date 08/07/2021
- Kim, D., KIm, J. and Kim, S. (2013)"A malicious application detection framework using automatic feature extraction tool on Android market." in Proc. of the 3rd International Conference on Computer Science and Information Technology, ICCSIT , 2013.
- Kubovic,O.(2019). Security. Retrieved October 10, 2021 from https://www.welivesecurity.com/false - positive/false negative-expertseurity.

- Kurniawan, H., Rosmansyah, Y and Dabarsyah, B.(2015).Android anomaly detection system using machine learning classification.In Electrical Engineering and Informatics (ICEEI), 2015 International Conference on, pages 288–293, Aug 2015.doi: 10.1109/ICEEI.2015.7352512.
- Meng, X. & Spanoudakis, G. (2016). MBotCS: A mobile botnet detection system based on machine learning. Lecture Notes in Computer Science, 9572, pp. 274-291. doi: 10.1007/978-3-319-31811-0_17
- Mesevage, S. (2019). What is an Intrusion System? Retrieved 07/08/2021from https://www.techopedy.com.
- Miller, S (2018). The Role of Machine Learning in Botnet Detection. Jamaica curtis.busbyearle@uwimona.edu.j
- Motylinski, M., MacDermott, A., Iqbal, F., & Shah, B.(2022). A GPU-based machine learning approach for detection of botnet attacks. Computers & Security 123(2022)1102918
- Mudassir , M., Unal , D.,Hammoudeh ,M., and Azzedin, F(2022). Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches. Wireless Communications and Mobile Computing Volume 2022, Article ID 2845446, 12 pages ttps://doi.org/10.1155/2022/2845446
- Negera, W.G.; Schwenker, F.; Debelee, T.G.; Melaku, H.M.; Ayano, Y.M(2022). Review of Botnet Attack Detection in SDN-Enabled IoT Using Machine Learning. Sensors 2022, 22, 9837. https://doi.org/ 10.3390/s2224983
- Rasheed, M.M., Alaa K. Faieq,A.K. , Ahmed A. Hashim, A.A (2019). Android Botnet Detection Using Machine Learning. International Information and Engineering Technology Association Vol.25 No 1 PP127-130,https://doi.org/10.18280/isi.://
- Sherif, A. (2024). Market Share of Mobile Operating Systems worldwide 2009 - 2024 by quarter.https://www.statista.com/aboutus/our-research-commitment/2657/ahmed-sherif
- Sri, R., Moorthya, S, and Nathiyab, N. (2023). Botnet Detection Using Artificial Intelligence. International Conference on Machine Learning and Data Engineering Botnet Detection Using Artificial Intelligence. ScienceDirect Available online at www.sciencedirect.com Procedia Computer Science 218 (2023) 1405–1413
- Statcounter(2021). Android Market Share in Nigeria. https://gs.statcounter.com/os-market-share/mobile/nigeria : Retrieved 08/07/2021
- Tariq, F. and Baig, S.(2017). Machine Learning Based Botnet Detection in Software Defined Networks Repository. International Journal of Security and Its Applications Vol. 11, No. 11 (2017), pp.1-12 http://dx.doi.org/10.14257/ijsia.2017.11.11.01 ISSN: 1738-
- Vuleta, B. (2023). 44 Worrying Malware Statistics to Take Seriously in 2021. Retrieved 08/07/2023 from:https://legaljobs.io/blog/malware-statistics/
- Yerima, S. Y., Alzaylaee, M.K., Shajan, A., & Vinod, P (2021). High Accuracy Detection of Mobile Malware Using Machine Learning. *Electronics* 2021, *10*(4), 519 https://doi.org/10.3390/electronics10040519