International Journal of Engineering and Artificial Intelligence

Journal home page: http://www.ijeai.com

A Comparative Experimental Evaluation of Antimalware Tools on Android Mobile Device

S. O Subairu[1], S. A. Gbadamosi[2]

[1,2] Cyber Security Science, Federal University of Technology Minna, Nigeria.

Corresponding Author: Islam4life@futminna.edu.ng

Original article Received 3 September 2023, Accepted 29 September 2023, Available online 1 December 2023

ABSTRACT

Information Security experts have been focusing on the study of malwares detection because of its rise recently. Android is the overwhelmingly dominant mobile operating system on the African phone market with 85.88%, while iOS, Series 40, Windows and other Operating systems has 8.84%, 0.57%, 0.39% and 3.23% respectively. Cybercriminals uses various types of malware to attack and compromise android devices in the recent years with the intent of getting access to sensitive information present in the victim's devices. Various detection tools exits in the market, but how reliable in terms of performance were put to experimental analysis in this work. Five antimalware tools and eight malwares were used for our analysis under a virtual environment. Results of our analysis shows kaspersky antimalware as best performed while 360 Total Security as least performed as it failed to detect any of the malware samples despite its high rating performance in apps store.

Keywords: Cybercriminals, Android, Antimalware, Malware, Mobile device.

1. Introduction

Malware is software's that disrupt, destroy or harm computers, mobile devices, networks, and other associated resources. Malware is transmitted on mobile devices or computers, without the awareness of their users. The most common tool used to propagate malware is networks and portable devices. Malware still constitutes a potential threat to the digital world, but with the growing use of the mobile phones and internet, the effect of malware on privacy, economy is severe and cannot be overlooked (Tahir, R., 2018).

Research firms projected market share for African-based Smartphone's, estimating about 68.85 percent of Smartphone's that are running android are sold from the middle of 2013 to nearly 75 percent in 2017.This appeals for security threats and attacks to be prevented. Not only has the Android OS become a key player on the mobile device market, but it has also become an attractive prospect for cyber criminals.

A significant source of privacy and security concerns in Android is users' ability to download third-party applications from alternative sources that do not review applications submitted to them for security testing to determine if the software contains malicious codes, as it did in the official Android Appstore (Ali M, et al, 2017).

2. Problem Statement

Cyber security global ranking done by Kaspersky in year 2019, ranked Nigeria as third in the world as shown in table 1, where Android mobile device users were attacked by mobile malwares with 37.72%, which has a gross effect on the economy of this nation.

Most android device users in Nigeria are affected by malware attacks and are faced with the challenges on how to overcome the attack and selecting the most suitable tool to fight this attack out of the numerous numbers of tool on the internet (Techeconomy, 2019).

Table 1. Global Ranking of Android Mobile Attack

Country*	%**
Iran	44.24
Bangladesh	42.98
Nigeria	37.72
India	36.08
Algeria	35.06
Indonesia	34.84
Pakistan	32.62
Tanzania	31.34
Kenya	29.72
Philippines	26.81

3. Malware Detecction Techniques

The classification and relationship between malware analysis and detection methodologies are shown on table 2, each malware detection strategy can be static, dynamic or hybrid, and the specification-based detection method is additionally inferred from heuristic-based detection techniques.

Table 2. Merit and Demerit of Malware Detection Methodologies

Malware Detection Techniques	Merits	Demerits
1. Signature based	-It is easy to detect known malware. - Uses fewer resources than other techniques.	- Unknown malwares cannot be detected.
2. Heuristic based	-Ability to detect known and unknown recent malware	-New and unknown malware information must be changed. - You need more time and space resources. - False-positive levels are high.
3. Specification based	-Ability to detect known, unknown, and new. Malwares. -false positive levels are low	- False-negative level is high. – Inefficient in modern malware detection. - The specification development takes time.

4. Literature Review

Smartphone. The success achieved on the desktop by their peers has incredibly added to increasing the level of assurance that mobile clients have procured. Types of renowned antiviruses are Avast, AVG, Norton, 360 Total

Security, F-Secure. The rapid evolution of malicious software provides Antivirus with new constraints. Similar to desktop platforms, their proficiency is closely related with their strategies of detection. (Felt, A.P et al, 2011) Categorizes these approaches into three classes: Form analysis, integrity checking and dynamic behaviour analysis.

Form Analysis: detects the existence of a threat in an application by static character. It may be focused on the research of signature, heuristics or spectral analysis.
Research of Signature: Looking for patterns or bits that are features of a known threat. Its main drawback is that it cannot detect unknown threats and known threats that are altered. It requires that the signature database be permanently updated. It is easy to implement and most commonly used in antivirus companies (Zhou, Y., & Jiang, X. 2012).
Spectral Analysis: Scrutinizes statements that are widely used by samples of malware, but uncommon in normal applications. To detect unknown threats, the frequency of such statements is analysed statistically. This method is susceptible to false positives, i.e. normal applications that are classified incorrectly as malware.
Heuristic Analysis: This approach is to establish and maintain rules that are used as a pattern to identify malicious applications. Like the previous approach, it is also subject to false alerts.

Integrity Checking: Is based on evidence that an abnormal file modification may reveal contamination by unsafe code. Dynamic behaviour analysis is used to screen an application's actions while it is running.

Dynamic Analysis: This third approach detects suspicious actions such as attempted modification of data from another application or modification of libraries and memory space reserved for the system.

Multi-Level Anomaly Detector for Android Malware (MADAM) is a proposed malware detection technique that tracks Android to detect actual malware infections at both kernel and user level. MADAM uses machine learning methods to differentiate between standard and malicious behaviours. MADAM's first prototype for Android Smartphone's has been implemented but its theoretical approach may also be applied to other mobile Operating Systems (OS) (G. Dini et al., 2012)

Zhou, H. (2019) Proposed an innovative method that uses neural network with a combined feature (static and dynamic) to determine whether the executable portable file is malicious or benign. The first form of neural network they use is a recurrent neural network trained to extract PE file behavioural features, and the second type is a convolutionary neural network used to categorize samples. This approach discovers malware by classifying images generated using a designed model (Zhou, H., 2019).

Another malware detection technique was proposed, which is named Hindroid. It determine the importance of different meta-paths, it uses a multi-kernel learning algorithm to automatically learn the weights of different data similarities. Promising experimental results indicate that HinDroid outperforms alternative malware detection methods for Android as well as popular mobile security products. HinDroid has now been integrated into the scanning tool of the Comodo Mobile Security product (Shifu Hou, Y. Y et al., 2017)

Burguera, I., & Zurutuza, U. (2011) Proposed a technique which they named Crowdroid for detecting android malware. It uses anomaly-based detection. However, their method was kind of different. CrowDroid used two types of dataset, the first is artificial malware created for test purposes and another from actual malware. The research presumed that detecting malware through checking system calls would work for rising and modern pernicious software..

Another method for identifying android malwares is through the use of machine learning procedures proposed by (Ali et al., 2017). It is said to be a practical and efficient malware detection framework with an accentuation on Android's mobile computing platform. An Android gadget has mounted a dataset consisting of both benign and pernicious software to assess behavioural patterns. The discoveries and estimates of this method's tests appeared that Random Forest and Support Vector Machine conveyed an excellent result among the algorithms examined.

Furthermore, The Author proposes a new hybrid approach for detecting mobile malware through both static and dynamic analysis. This technique is universal, which can effectively detect various types of malware. They used malware samples and mild applications using net link technology to produce patterns of system calls related to file and network access. They also build up a malicious pattern set and a normal pattern set by comparing malware patterns with benign applications (Tong, F., & Yan, Z. (2017). The related woks with methodology result and limitation is being shown in table 3.

Table 3. Related Works

S/N	Author	Methodology	Result	Limitation
1.	Ali, et al., (2018)	Heuristic based (Anomaly) Detection Technique.	The findings and comparisons from the experiments of this method showed that among the algorithms examined, Random Forest and Support Vector Machine delivered the best result.	It hardly detects newly launched malwares.
2.	Tong,F., Yan, Z. (2017)	Hybrid (static + dynamic) Detection Technique.	The proposed technique outperforms its counterpart in terms of detection techniques on mobile applications with greater accuracy of detection rated for various typesof malware.	i. It is presently made for only android operating system. ii. It is necessary to innovate a new approach to efficiently fuse data collected on mobile devices to improve the efficiency of malware detection for both communication and computation costs.
3.	Shifu et al. (2017)	Proposed heterogeneous information network (HIN)	Promising experimental results show that HinDroidperforms better than other techniques for detection of malwares on Android and popular mobile security products.	
4.	Zhou, H. (2015)	(Static + dynamic) and Neural networks	This method has the ability to detect unknown malicious samples.	
5.	Burguera, I., Zurutuza, U. (2014)	Heuristic based (Anomaly) Detection Technique.	It can distinguish between harmless and harmful applications of the same name and version, and it can detect anomalous behaviour of known applications.	Faced with the difficulty of persuading the Android user community to install the Crowdroid application.
6.	(G. Dini et. al, 2012)	Heuristic based (Anomaly) Detection Technique.	MADAM's first prototype detects several real malwares in the wild. With the rate of false positives yielded after the learning phase, MADAM does not affect the system usability.	Further extension of this framework, which combines a global monitoring approach with more specific monitors that consider additional features.

5. Methodology

Five antimalware tools were used, namely: Avast, 360 Total Security, AVG Antivirus, Kaspersky, and Norton. This selection was based on a user survey on antimalware that are often used. The result obtained from the survey study is shown on Figure 1.

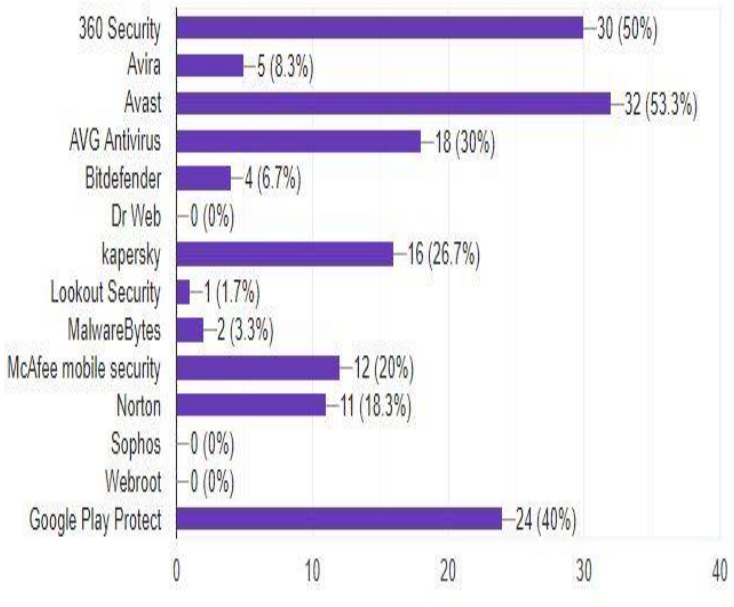

Figure 1. User's Experience of Anti-Malware Tools

Eight malware samples were used in the experiment, which were all gotten from malware repository of Github and Total Virus. These malware samples are Angry Birds, Advance File Manager, Dovizcevirici, Opera Mini, Password Saver, Secret SMS, Trust Mobile and 156.YilMobil.

Github is an open source platform for sharing and storing source codes, new technology, as well as tools. Malware samples are shared in compressed (zipped) files form.

Virus Total is famous malware repository owned by Google. This repository stored malware samples collected over time and Researchers are given access for the purpose of research only.

Five Systems with Specifications of: Windows 10 Pro Operating System, installed memory (RAM) – 4 GB, Processor – Intel (R) Core i5-2520 CPU @ 2.50GHz, System type – 64-bit Operating System, x64 based processor were used.

BlueStacks is an App Player tool for running Android apps on a personal computer. Having interface for managing all features on a virtual device.

Experimental Procedures

The procedures for the experiment were as follows:

i. Survey study to obtained users most used antimalware tools

ii. Installation of Bluestack on each of the five systems

iii. Installation of the five antimalware; each per system

iv. Downloading/scanning of each of the malware on each of the system

v. Result obtained and analyze

vi. System reset

vii. Back to step (2) for the next malware until the eight samples malwares have been exhausted

viii. Experiment closed

The pictorial view of the experiment procedure is shown in Figure 2.

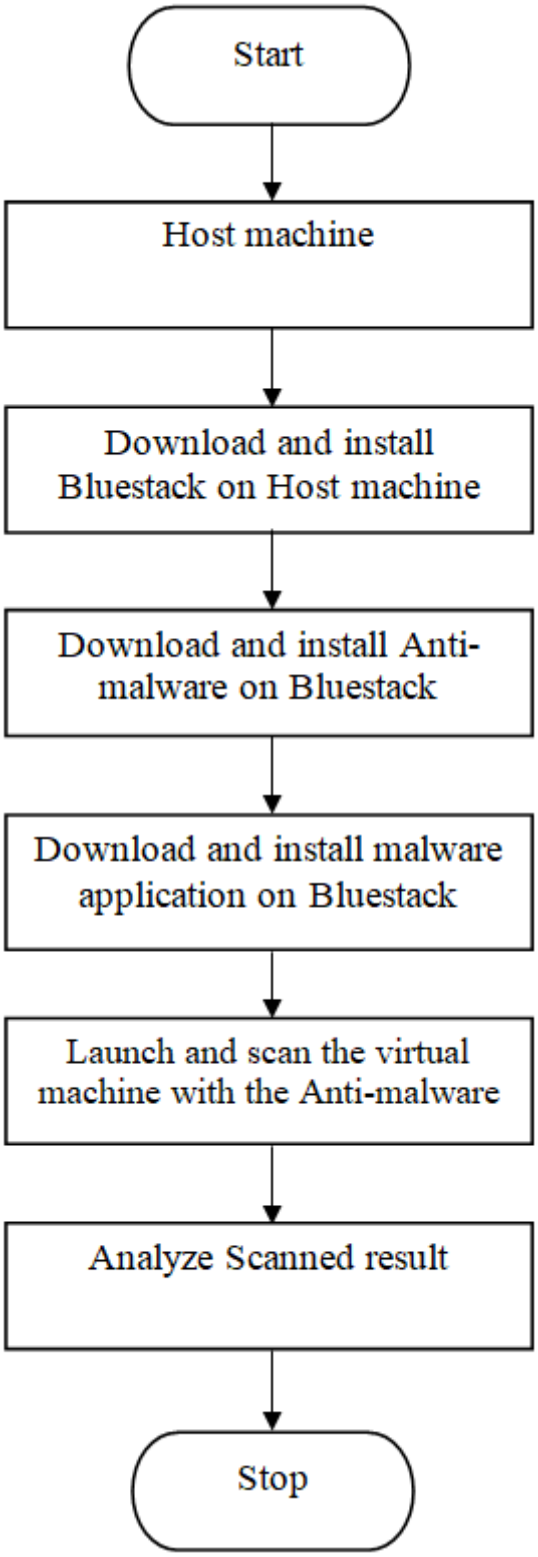

Figure 2. Experimental procedure flow chart

6. Analysis

The followings were the results obtained from the experimental analysis of five malware detectors on eight malwares. Each table represents each of the antimalware tools, which show its ability to either, detect or failed to detect malware.

Avast

Table 4. Result of Avast Anti-Malware Tool.

S/N	Malwares	Detected
1.	Angry Birds	No
2.	Advance File Manager	Yes
3.	DovizCevirici	No
4.	Opera Mini	No
5.	Password Saver	No
6.	Secret SMS	Yes
7.	Trust Mobile	Yes
8.	156. YilMobil	Yes

Total Security

Table 5. Result of 360 Total Security Anti-Malware Tool

S/N	Malwares	Detected
1.	Angry Birds	No
2.	Advance File Manager	No
3.	DovizCevirici	No
4.	Opera Mini	No
5.	Password Saver	No
6.	Secret SMS	No
7.	Trust Mobile	No
8.	156. YilMobil	No

AVG Anti-Virus

Table 6. Result of AVG Anti-Malware Tool.

S/N	Malwares	Detected
1.	Angry Birds	No
2.	Advance File Manager	Yes
3.	DovizCevirici	No
4.	Opera Mini	No
5.	Password Saver	No
6.	Secret SMS	Yes
7.	Trust Mobile	Yes
8.	156. YilMobil	Yes

Kaspersky

Table 7. Result of Kaspersky Anti-Malware Tool.

S/N	Malwares	Detected
1.	Angry Birds	No
2.	Advance File Manager	Yes
3.	DovizCevirici	Yes
4.	Opera Mini	No
5.	Password Saver	No
6.	Secret SMS	Yes
7.	Trust Mobile	Yes
8.	156. YilMobil	Yes

Norton

Table 8. Result of Norton Anti-Malware Tool.

S/N	Malwares	Detected
1.	Angry Birds	No
2.	Advance File Manager	Yes
3.	DovizCevirici	No
4.	Opera Mini	No
5.	Password Saver	No
6.	Secret SMS	Yes
7.	Trust Mobile	Yes
8.	156. YilMobil	Yes

The presented tables' shows that Kaspersky antimalware perform best as it detect five out eight samples malware while 360 Total Security was the least perform antimalware tool since it failed to detect any of the samples malware as shown in Figure 3.

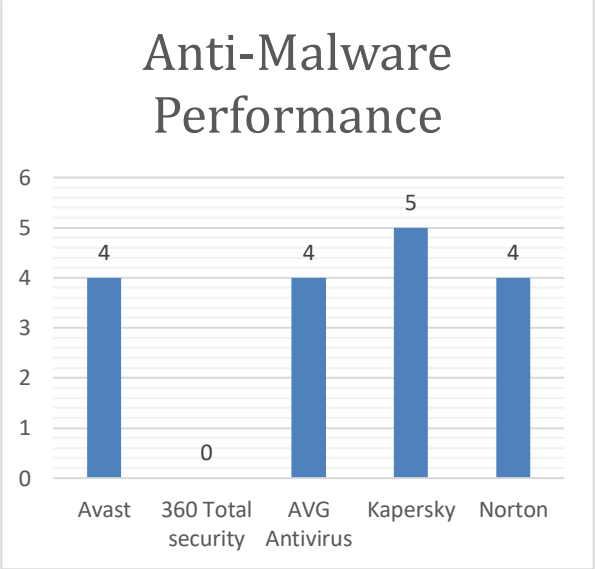

Figure 3. Overall Performance of Malware detector Tools

7. Conclusion

The summary of this research as shown in Figure 2 vividly point out the best and the poorest performed anti-malware tool as they were tested on eight types of android malwares. Avast , AVG Antivirus and Norton ware able to detect four of the eight samples malware, while 360 Total Security failed to detect any of these malwares. These four anti-malwares (Avast, AVG Anti-virus, Kapersky and Norton) detect these malwares respectively when the malware is being installed on the mobile device.

From this research, one can equally conclude that playstore rating of tools in terms of performance may be misleading sometimes. This was established as in the case of 360 Total Security Anti-malware tool, that was rated 4.6 as shown in Table 9, and yet failed to detect any of the samples malwares.

Table 9. Performance Rating of Anti-Malware Tools by Google Playstore.

S/N	Anti-malware tools	Rating
1.	Avast	4.7
2.	**360 Total Security**	***4.6**
3.	AVG Anti-virus	4.7
4.	Kaspersky	4.9
5.	Norton	4.7

References

Tahir, R. (2018). A Study on Malware and Malware Detection Techniques. International Journal of Education and Management Engineering, (March), 20–30. https://doi.org/10.5815/ijeme.2018.02.03

Ali, M. Al, Svetinovic, D., Aung, Z., & Lukman, S. (2017). Malware Detection in Android Mobile Platform using Machine Learning Algorithms. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 763–768.

Techeconomy. (2019). Nigeria Now Ranks Third On Mobile Malware Attacks From Fifth In 2017. Retrieved November 6, 2019, from https://techeconomy.ng/2019/03/07/nigeria-now-ranks-third-on-mobile-malware-attacks-from-fifth-in-2017/

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '11, 3. https://doi.org/10.1145/2046614.2046618

Zhou, Y., & Jiang, X. (2012). Dissecting Android malware: Characterization and evolution. Proceedings - IEEE Symposium on Security and Privacy, (4), 95–109. https://doi.org/10.1109/SP.2012.16

G. Dini, F. Martinelli, A. Saracino, D. S. (2012). MADAM: a Multi-Level Anomaly Detector for Android Malware. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, 240–253.

Zhou, H. (2019). Malware Detection with Neural Network Using Combined Features. In China Cyber Security Annual Conference, 96–106. https://doi.org/10.1007/978-981-13-6621-5

Shifu Hou, Y. Y., Song, Y., & Abdulhayoglu, M. (2017). HinDroid : An Intelligent Android Malware Detection System Based on Structured Heterogeneous Information Network. Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1507–1515. https://doi.org/10.1145/3097983.3098026

Burguera, I., & Zurutuza, U. (2011). Crowdroid : Behavior-Based Malware Detection System for Android. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 15–26. https://doi.org/10.1145/2046614.2046619

Ali, M. Al, Svetinovic, D., Aung, Z., & Lukman, S. (2017). Malware Detection in Android Mobile Platform using Machine Learning Algorithms. 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 763–768.

Tong, F., & Yan, Z. (2017). A hybrid approach of mobile malware detection in Android. Journal of Parallel and Distributed Computing, 103, 22–31. https://doi.org/10.1016/j.jpdc.2016.10.012