PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 2 [August, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

A COMPARATIVE STUDY OF ANTIVIRUS PERFORMANCE AGAINST ANDROID MALWARE

NUR SYAQIRAH IWANI ROSLI
College of Computing, Informatics and Mathematics, Campus Jasin, Jasin, Melaka
2021853872@student.uitm.edu.my

ALYA GEOGIANA BUJA*
College of Computing, Informatics and Mathematics, Campus Jasin, Jasin, Melaka
geogiana@uitm.edu.my

Article Info

Abstract

This study investigates the effectiveness of five antivirus programs (Kaspersky, AVG, McAfee, TrendMicro, and Bitdefender) on Android devices, focusing on key performance metrics such as detection rates, battery usage, storage management, and operating temperature. Employing a mixed-methods approach, the research combines qualitative and quantitative data to provide a comprehensive assessment of each antivirus program's capabilities. The findings reveal that Kaspersky and AVG excel in detection rates while maintaining efficient energy usage and low device temperatures. Conversely, McAfee exhibits higher power consumption and lower detection rates, and TrendMicro and Bitdefender, despite good detection capabilities, result in increased device temperatures. The study concludes that selecting antivirus software requires a balanced evaluation of protection efficacy and operational efficiency, highlighting the importance of diverse device testing and the integration of advanced performance assessment tools in future research.

Keywords: Antivirus effectiveness, Android devices, detection rates, battery usage, storage management, operating temperature, Kaspersky, AVG, McAfee, TrendMicro, Bitdefender, mixed-methods approach, protection efficacy, operational efficiency, performance assessment, malware impact.

Received: August 2024
Accepted: March 2025
Available Online: August 2025

INTRODUCTION

The research highlights Android malware's growing threat and the significance of antivirus software for device security. The evolving technology in Android has attracted malware writers, who continuously develop malicious applications to breach device security for financial gain (Ashawa & Morris, 2019). Antivirus software is an important tool for protecting Android devices from malware attacks. However, not all antivirus software is created equal.

Some antivirus systems struggle to detect and prevent Android malware due of its evolving nature. The project includes a background, problem definition, purpose, and significance, contributing to Android malware antivirus development. The study emphasises the importance of comparing antivirus products to better safeguard Android devices from malware attacks. Comparative studies of antivirus performance against Android malware are important because they can help users to choose the best antivirus software for their needs and to be aware of the strengths and weaknesses of different antivirus software products. Malware not only violates the security and privacy of computer users, but it can also result in significant financial loss and in the denial of critical services. (Trivikram Muralidharan, 2022)

The first problem statement is that antivirus software is ineffective at detecting and blocking Android malware. Besides, with malware techniques constantly evolving, manual malware analysis couldn't keep pace with the evolving attack strategies. (Yue Liu, 2022). The final statement in this project is antivirus software vendors are failing to protect Android users from malware. There are considerable technical obstacles. The process of creating antivirus software that works well is difficult and complex.

This project have two objective: To evaluate five selected antivirus programs based on detection rates, system impact, and effectiveness and to compare five selected antivirus programs to determine which one offers the best balance of performance. This proposal only targeted the Android platform with the specific aim of countering a wide range of malicious software, such as worms, viruses, Trojans, ransomware, and spyware. In order to tackle these potential dangers, the study assessed the efficacy of five antivirus software: AVG Antivirus, Kaspersky, Trend Micro, Bitdefender, and McAfee. The sophistication and number of Android malware threats have increased significantly in recent years, prompting the need for effective antivirus solutions. Despite the presence of numerous antivirus programs, not all are equally effective, and a comparative study is necessary to identify the most efficient ones .

LITERATURE REVIEW

The literature review examines different methodologies used by antivirus companies and discusses their strengths and weaknesses. The chapter also points out a consensus in the literature that current antivirus tools are often inadequate in dealing with the rapidly changing nature of Android malware.

Network Security

Our data, networks, and privacy are continually threatened by cybercriminals looking for vulnerabilities. Network security—the digital world's guardian angel. It shields our sensitive data from theft, disturbance, and unauthorised access. Also, networks make attacks on applications possible by delivering unwanted traffic or leaking sensitive data. (Zave & Rexford, 2021). Why is network security crucial? Imagine sensitive data stolen, hackers causing financial losses, crippled systems hurting organizations, and reputational damage. A cyber-attack is a relatively new idea that comprises a wide range of criminal operations that can be carried out by exploiting the capabilities of today's advanced information and communication technologies. (Albahar, 2019). Hacking. Consequently, illicitly acquiring confidential information such as passwords, usernames, banking data, and other personal particulars. Malicious hackers utilised the pilfered data to carry out unauthorised withdrawals from individuals' accounts. (Alawida et al., 2022). Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. (B. Savant & D. Kasar, 2021). Additionally, it detects any internal or external network entry points. (El Alaoui & Gahi, 2020)

Smartphone and Mobile application

Smartphones have transcended their humble beginnings as communication devices to become indispensable mini-computers in our palms. They hold our personal and professional lives within their screens, from banking apps and social media to work documents and entertainment. Mobile devices essentially have a big impact on cyber security since the kind of data that is stored and accessed on them increases the security concerns. (Zheng, 2022). To fully grasp the security aspects of Android, one must have a comprehensive understanding of the entire stack of technologies employed by the Android Open-Source Project (AOSP) (Mos & Chowdhury, 2020). However, the majority of security features are offered by the operating system and comprehending them necessitates a thorough understanding of operating systems, runtime environments, and networks.

Android incorporates a range of security features to protect users and their data. For example, Android Security Threats: The Android operating system employs a permission-based approach to regulate and oversee the access of third-party Android applications to important resources, ensuring security. (Ahmed & Sallow, 2017). Secondly, kernel-Based Application Sandboxing: The kernel-based application sandbox assigns distinct User IDs (UIDs) and Group IDs (GIDs) to each application. This hinders the ability of programmes to access data belonging to other applications. According to (Asamoah, 2021) Antivirus (AV) software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. It protects against viruses, worms, trojans, ransomware, spyware, and other malware.

Smartphone and Mobile application

According to (Asamoah, 2021) Antivirus (AV) software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. It protects against viruses, worms, trojans, ransomware, spyware, and other malware. AVG Antivirus is a series of antivirus software created by AVG Technologies, a division of Avast Software. It provides defence against viruses, malware, ransomware, spyware, and other digital hazards. Kaspersky Antivirus is a line of antivirus software developed by Kaspersky Lab, a Russian cybersecurity company. The product was first released in 1997 and has since become one of the most popular antivirus programs in the world. Bitdefender Antivirus is a line of antivirus software developed by Bitdefender, a Romanian cybersecurity company. The product was first released in 2001 and has since become one of the most popular antivirus programs in the world. Bitdefender Antivirus offers protection against viruses, malware, ransomware, spyware, and other online threats. McAfee Mobile Security is a comprehensive mobile antivirus app that safeguards your Android device from a wide range of online threats. It offers real-time protection against viruses, malware, ransomware, spyware, and other online threats. Trend Micro Antivirus is a line of antivirus software developed by Trend Micro, a Japanese cybersecurity company. The product was first released in 1988 and has since become one of the most trusted antivirus programs in the world. AVG Antivirus is a series of antivirus software created by AVG Technologies, a division of Avast Software. It provides defence against viruses, malware, ransomware, spyware, and other digital hazards.

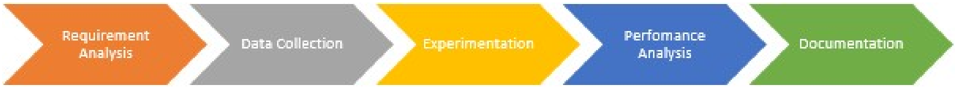
Introduction to Android Malware

According to (Mos & Chowdhury, 2020) Android malware is a piece of code with the intent to cause harm or steal information of the victim using an Android OS device. No one can get hold of APKs for any Android app because the Android OS is an Open Source operating system. Because of this, the Android OS is very risky. With just one click, you could download something that gives you full access to your phone and lets you see all of your files and photos.Self-replicating and spreading independently, 'Selfmite' is an example of an Android worm that propagated through SMS, enticing users to click a link and inadvertently install malicious software. According to (Piccione et al., 2023) One of the primary methods for defending against malware is using antivirus software, designed to detect and remove malicious code. However, the increasing sophistication of malware presents a significant challenge for antivirus software to keep pace.

These forms of malware share the potential to cause rapid infection, leading to network congestion and, consequently, performance degradation on Android devices. (S B et al., 2019). Infecting legitimate files or apps, the 'Gunpoder' malware serves as an example by compromising APK files. This infiltration enables attackers to take control of the device and pilfer sensitive information. The impact on Android devices includes file corruption, unauthorized access, and the potential for spreading to other apps. Disguised as legitimate software to deceive users, 'Android.Fakeapp' serves as an example by posing as a banking app. This deceptive tactic tricks users into entering sensitive financial information. Encrypting user files and demanding a ransom for decryption, 'DoubleLocker' serves as an example by encrypting files and altering the device's PIN. This malicious action demands a ransom in cryptocurrency for recovery.Secretly gathering user data without consent, 'Exodus' serves as an example by silently collecting sensitive information, including contacts, messages, and call logs. This is malicious software that is installed on the victim’s machine without his knowledge, and it is used to monitor and collect information about a particular user.

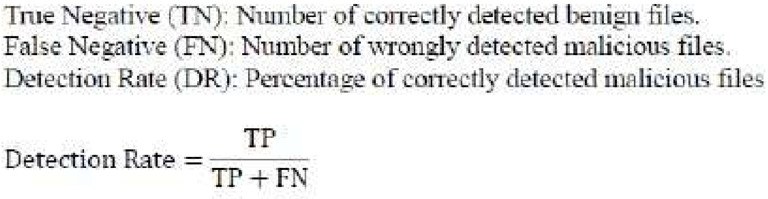
METHODOLOGY

The five phases of this process were requirement analysis, data collection, experimentation, performance analysis, and documentation shows in figure. Each phase was crucial to project success. The requirement analysis step defined the experiment's demands and goals. Relevant data and metrics were collected methodically. Antivirus programme testing were performed during experimentation. Performance analysis assessed and interpreted results to measure antivirus programme efficacy and efficiency. Finally, detailed recording of findings, methods, and conclusions was necessary. These steps were carefully detailed to assure experimentation success in this project.



The number of experiments refers to the number of attempts made. Five antivirus software instances conducted scans to detect a single infection. The purpose was to assess accuracy, false positives, false negatives, as well as the impact on battery, storage, and temperature. In addition, the experiment involved the use of two phones, which led to a total of 500 tests, calculated by multiplying 5 (Malware) x 5 (Antivirus) x 10 (Testing) x 2 (Phones). The activities included monitoring and logging detection rates, system impact, and efficacy in detecting malware on Android devices. Simulated malware was used to evaluate the effectiveness of antivirus systems, and data gathered during tests was thoroughly collected and organised. The next phase entailed thoroughly analysing and interpreting the results to determine relevant conclusions. The deliverables comprised recorded installs of selected antivirus programmes on Android devices, an assessment of their performance in detecting and mitigating simulated malware, and a thorough dataset compiled throughout the experimental phase.

This experimentation incorporates calculations of detection rates from previous studies to compare and evaluate the findings versus existing results. The goal is to use these existing computations to offer a thorough study of antivirus performance and confirm experimental results



True Negative (TN): Number of correctly detected benign files.
False Negative (FN): Number of wrongly detected malicious files.
Detection Rate (DR): Percentage of correctly detected malicious files

$$\text{Detection Rate} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

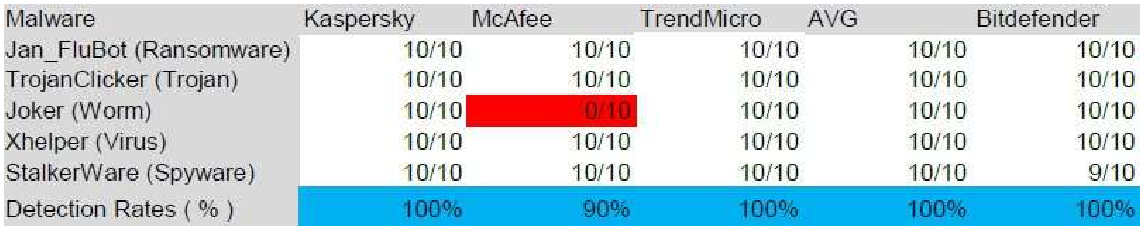
Figure 3. 4 Calculation on Detection Rates

(Altaher et al., 2011)

The documentation phase was the final step in the antivirus vs. malware framework comparison, and it included the recording of all information and analysis gathered during the project. This compilation of observations proved to be an invaluable resource for future application-related efforts. Following the completion of documentation, the Final Report was methodically prepared for presentation, using the study findings as a standard to evaluate the project's success. This phase's activities included defining the overall project development and combining material from each phase to create thorough documentation.

RESULT AND DISCUSSION

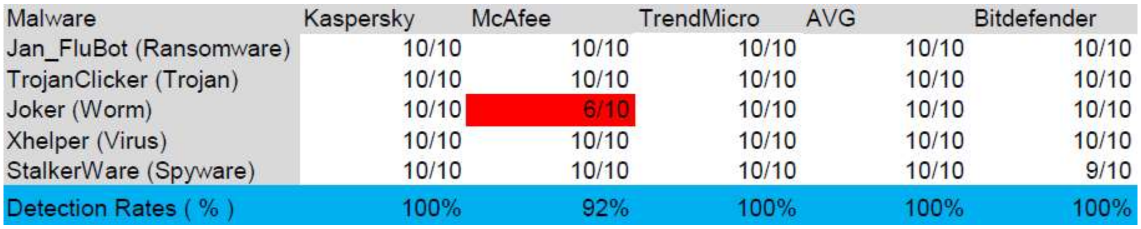
The results of the comparative study of antivirus performance against Android malware. The chapter discusses the accomplishment of the study's two main objectives: evaluating five selected antivirus programs (Kaspersky, Bitdefender, TrendMicro, AVG, and Avast) based on detection rates, system impact, and effectiveness, and comparing these programs to determine which offers the best balance of performance. This project also use two different phone in conducted this experimentation. The comprehensive experiment conducted with these antivirus programs against different types of malware is detailed, with a focus on identifying the best-performing antivirus in terms of detection rates and overall effectiveness. The results highlight the strengths and weaknesses of each antivirus program, providing insights into their performance in real-world scenarios.



Malware	Kaspersky	McAfee	TrendMicro	AVG	Bitdefender
Jan_FluBot (Ransomware)	10/10	10/10	10/10	10/10	10/10
TrojanClicker (Trojan)	10/10	10/10	10/10	10/10	10/10
Joker (Worm)	10/10	0/10	10/10	10/10	10/10
Xhelper (Virus)	10/10	10/10	10/10	10/10	10/10
StalkerWare (Spyware)	10/10	10/10	10/10	10/10	9/10
Detection Rates (%)	100%	90%	100%	100%	100%

Figure 2 Detection Rates on xiaomi

The figure 2 illustrate the detection rates of various antivirus software, specifically Kaspersky, TrendMicro, AVG, Bitdefender, and McAfee, against different types of malware. According to the overall detection rates, Kaspersky, TrendMicro, AVG, and Bitdefender each achieved a perfect score of 100%, indicating their high effectiveness in identifying malware. In contrast, McAfee lagged behind with a detection rate of 90%.



Malware	Kaspersky	McAfee	TrendMicro	AVG	Bitdefender
Jan_FluBot (Ransomware)	10/10	10/10	10/10	10/10	10/10
TrojanClicker (Trojan)	10/10	10/10	10/10	10/10	10/10
Joker (Worm)	10/10	6/10	10/10	10/10	10/10
Xhelper (Virus)	10/10	10/10	10/10	10/10	10/10
StalkerWare (Spyware)	10/10	10/10	10/10	10/10	9/10
Detection Rates (%)	100%	92%	100%	100%	100%

Figure 3 Detection Rates on Honor Play

The figure 4.5 contrasts the efficacy of a variety of antivirus software, including Kaspersky, McAfee, TrendMicro, AVG, and BitDefender. Kaspersky has a 100% detection rate, which is indicative of its exceptional ability to identify threats. On the other hand, McAfee's detection rate is slightly above 90%, which implies that it is less effective than other antivirus programmes.

Battery Usage

The study conducted a detailed analysis of battery usage for the antivirus programs across the two phones, Xiaomi 6A and Honor Play. For the Xiaomi 6A, Kaspersky and AVG emerged as the most efficient in terms of battery consumption, maintaining consistently low usage across various malware types. In contrast, McAfee exhibited the highest battery consumption, particularly with TrojanClicker (Trojan) and StalkerWare (Spyware), indicating less efficient power management.

For the Honor Play, AVG and TrendMicro showed consistent and generally lower battery usage, suggesting better optimization and resource management. On the other hand, McAfee's battery usage was notably high when dealing with the Joker (Worm) malware, with consumption peaking at around 2.5%, making it the least efficient in this regard.

Storage Usage

Storage usage was another critical metric analyzed, with significant differences observed between the antivirus programs. For the Xiaomi 6A, TrendMicro consumed the most storage, particularly for Joker (Worm), reaching approximately 0.25%. This was followed by notable storage usage for TrojanClicker (Trojan) and StalkerWare (Spyware). AVG and Bitdefender exhibited similar storage usage patterns, with the highest being around 0.22% for StalkerWare (Spyware) and TrojanClicker (Trojan).

In the case of the Honor Play, all antivirus programs demonstrated low storage usage for Jan_FluBot (Ransomware), with values ranging between 0.02% and 0.04%. TrojanClicker (Trojan) also resulted in minimal storage usage across all tested programs, indicating efficient management of storage resources by these antivirus solutions.

Temperature

Temperature management was assessed to understand the impact of antivirus programs on device overheating. Kaspersky and AVG were able to maintain lower average temperatures, around 35°C and 36.4°C, respectively, indicating efficient processing and less thermal strain on the devices. Bitdefender and TrendMicro, however, displayed higher temperatures, reaching up to 39°C, likely due to the intensive processing required to handle complex malware. McAfee was identified as the least balanced in terms of performance, showing higher temperatures and greater battery usage, reflecting its less efficient handling of resources.

CONCLUSION

The conclusion of this study synthesizes the results from the comparative analysis of five antivirus programs—Kaspersky, AVG, Trend Micro, Bitdefender, and McAfee—on the Xiaomi 6A and Honor Play cellphones. This research aimed to evaluate the performance of these antivirus solutions across various metrics, including detection rates, battery usage efficiency, storage management, and operating temperature.

The findings revealed that Kaspersky and AVG stood out as the most balanced and effective antivirus programs. Both achieved high detection rates, effectively identifying and mitigating a range of malware threats. Additionally, they maintained efficient energy usage and low operating temperatures, ensuring that the devices remained protected without significantly draining battery life or causing overheating. These factors are crucial for enhancing user experience and prolonging device longevity.

Trend Micro and Bitdefender also demonstrated success in malware detection, performing well in identifying threats. However, these programs were associated with higher operating temperatures and increased power usage. While effective in providing security, their less efficient management of device resources could lead to quicker battery drain and potential overheating issues.

McAfee, in contrast, exhibited higher power consumption and lower detection rates compared to the other antivirus programs tested. This made McAfee less efficient overall, as it not only consumed more battery power but also provided less reliable protection against malware.

In summary, this study highlights the importance of a comprehensive evaluation of performance criteria when selecting antivirus software. The best antivirus programs, according to the project's findings, were Kaspersky and AVG. These programs offered the most effective combination of high detection rates, efficient battery usage, and low operating temperatures, making them the optimal choices for ensuring robust protection without compromising device performance .

References

Ahmed, O., & Sallow, A. (2017). Android Security: A Review. *Academic Journal of Nawroz University*, *6*(3), 135–140. https://doi.org/10.25007/ajnu.v6n3a97

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4), 993–1006. https://doi.org/10.1007/s11948-016-9864-0

Asamoah, H. (2021). *ANTIVIRUS SOFTWARE VERSUS MALWARE*. https://jarch.donnu.edu.ua/article/view/10531

Ashawa, M., & Morris, S. (2019). Analysis of Android Malware Detection Techniques: A Systematic Review. *International Journal of Cyber-Security and Digital Forensics*, *8*(3), 177–187. https://doi.org/10.17781/p002605

B. Savant, V., & D. Kasar, R. (2021). A Review on Network Security and Cryptography. *Research Journal of Engineering and Technology*, 110–114. https://doi.org/10.52711/2321-581x.2021.00019

El Alaoui, I., & Gahi, Y. (2020). Network Security Strategies in Big Data Context. *Procedia Computer Science*, *175*, 730–736. https://doi.org/10.1016/j.procs.2020.07.108

Liu, Y., Tantithamthavorn, C., Li, L., & Liu, Y. (2022). Deep Learning for Android Malware Defenses: a Systematic Literature Review. *ACM Computing Surveys*. https://doi.org/10.1145/3544968

Mos, A., & Chowdhury, M. M. (2020a, July 1). *Mobile Security: A Look into Android*. IEEE Xplore. https://doi.org/10.1109/EIT48999.2020.9208339

Mos, A., & Chowdhury, M. M. (2020b, July 1). *Mobile Security: A Look into Android*. IEEE Xplore. https://doi.org/10.1109/EIT48999.2020.9208339

Muralidharan, T., Cohen, A., Gerson, N., & Nissim, N. (2022). File Packing from the Malware Perspective: Techniques, Analysis Approaches, and Directions for Enhancements. *ACM Computing Surveys*, *55*(5). https://doi.org/10.1145/3530810

Piccione, A., Bernardinetti, G., Pellegrini, A., & Bianchi, G. (2023). *Is Your Smartphone Really Safe? A Wake-up Call on Android Antivirus Software Effectiveness*. https://www.alessandropellegrini.it/publications/Pic23.pdf

S B, C., A B, R., & G, N. S. (2019). A Research on Different Types of Malware and Detection Techniques. *International Journal of Recent Technology and Engineering*, *8*(2S8), 1792–1797. https://doi.org/10.35940/ijrte.b1155.0882s819

Zave, P., & Rexford, J. (2021). Patterns and Interactions in Network Security. *ACM Computing Surveys*, *53*(6), 1–37. https://doi.org/10.1145/3417988

Zheng, Y. (2022). International Journal of Sensor Networks and Data Communications Short Communication The Impact of Mobile Gadgets on Cyber Security. *The Impact of Mobile Gadgets on Cyber Security*, *11*(2090-4886), 2022. https://doi.org/10.37421/2090-4886.2022.11.158