A study to quantitatively evaluate global mobile antivirus and compare effectiveness

Youngrak Ryu*
KAIST Cyber Security Research Center
Daejeon, South Korea
yrryu@kaist.ac.kr

Kangsik Shin
KAIST Cyber Security Research Center
Daejeon, South Korea
ksshin90@kaist.ac.kr

Jeongho Lee
KAIST Cyber Security Research Center
Daejeon, South Korea
ddanzit@kaist.ac.kr

Dong-Jae Jung
KAIST Cyber Security Research Center
Daejeon, South Korea
jjp1018@kaist.ac.kr

Ho-Mook Cho‡
KAIST Cyber Security Research Center
Daejeon, South Korea
chmook79@kaist.ac.kr

***Abstract*—The study quantitatively evaluates the effectiveness of ten Android mobile antivirus products by developing standardized criteria across five key categories: functionality, resource efficiency, usability, additional features, and vendor support. The research measures detection accuracy, resource consumption, and overall usability through rigorous testing, including real-time detection, manual scans, and performance assessments. The results highlight notable variations in antivirus performance, with some excelling in detection rates while others are more resource-efficient. The study emphasizes the need for continuous updates and further research to refine these evaluation criteria, offering a data-driven approach to improving mobile antivirus solutions.**

***Index Terms*—Mobile antivirus, Android, Quantitative evaluation, Evaluation criteria, Mobile security.**

I. Introduction

The International Telecommunication Union (ITU) estimates that mobile subscriptions worldwide exceeded 8.9 billion in 2023, especially an increase of nearly 300 million subscriptions from the previous year due to the rise in smartphone users [1]. In the United States, adult smartphone users spent an average of 4 hours and 39 minutes per day in 2024, compared to 3 hours and 7 minutes per day watching television in 2022 [2]. As these statistics demonstrate, the smartphone has become an indispensable device. Users primarily use their smartphones for communication with other users, such as messaging services and sending emails, for economic activities, such as online banking and purchasing products, and entertainment, such as listening to music and watching videos [3]. Notably, traditional PC malware used to attack victims‘ PCs overlaps with mobile users' primary usage, and spontaneously, traditional malware developers are shifting their platforms to mobile and creating malware for mobile targets similar to their traditional methods. Figure 1 shows the number of mobile malware attacks on Kaspersky's antivirus from Q3 2022 to Q1 2024 [4]. In 2023, approximately 19 million attack attempts were detected, rising every quarter. According to Zimperium's report, 925,000 new mobile malware samples were detected in 2022, a 51% growth from the previous year, meaning 5% of Android smartphones were infected [5]. The major types of mobile malware are smishing via SMS or Messenger, adware that phishing and displays unwanted ads, spyware that steals personal information, and bank trojans that steal personal financial information, all of which target smartphone users' primary purpose of use. The prevalence of cybercrime against mobile devices is rising, leading to a growing concern among users. Consequently, there is a noticeable increase in the number of mobile antivirus installations on smartphones as users strive to protect their devices. This threat surge is reflected in the expansion of the commercial mobile antivirus market.

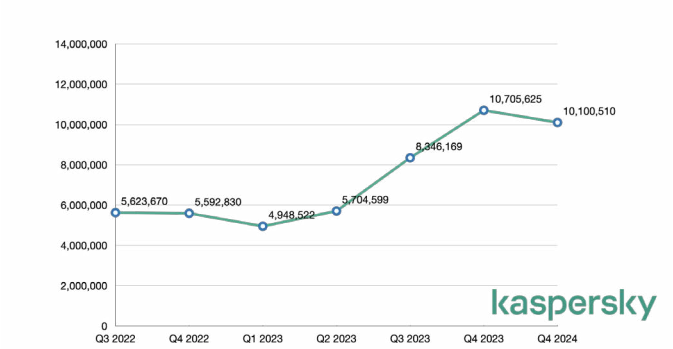

Fig. 1. Number of attacks targeting users of Kaspersky mobile solutions [4]

While about 30 antivirus products are listed on Google Play [6], the Android application market. There is a lack of metrics to evaluate the performance of commercial mobile antivirus products from the perspective of protecting users' devices from cyber threats. Vendors focus on promoting their products with additional features and price benefits rather than quantitative measures of antivirus detection performance. Therefore, users

This work was developed with the support of Global Cybersecurity Research grant (Project ID: 1711202451) from the Ministry of Science and ICT, Republic of Korea.

face a lack of information to help them differentiate and select the products with better performance and features from the wide range of products on the market. Antivirus testing institutions for PCs have been testing mobile antivirus products for several years and publishing the results. However, there is a lack of information about the detailed test items, test methods, and test samples, and previous studies either evaluate security software unsuitable for the new platform of mobile products or are outdated, and new evaluation metrics need to be developed. In this paper, we develop detailed evaluation metrics suitable for evaluating modern mobile antivirus products and apply them to ten Android mobile antivirus products to quantitatively evaluate the suitability of the evaluation metrics. This study aims to provide reliable evaluation results for various users and objective criteria for product selection.

II. Related Work

A. Android Antivirus

Android antivirus protects against hacker attacks and malicious app exploits by detecting and preventing these threats from attacking the user's device when malicious apps are installed or downloaded. Periodic scans protect the device by blocking malicious apps that have been installed inadvertently or unknowingly by the user [7]. Most antivirus vendors offer both free and paid models, with paid subscription models that add features such as VPN, privacy, file cleanup, and Wi-Fi network protection in addition to the mobile antivirus solution. Mobile antivirus use a combination of lightweight detection methods and external analytics due to limited resources compared to their PC version. The detection methods are categorized as follows.

1) Static Analysis: Static analysis, while a powerful tool, has its limitations. It detects malicious apps based on data analyzed without executing the code that performs the behavior. There are signature and permission analysis methods. Signature methods detect malware by analyzing known malware and patterning its attributes. Typical static attributes analyzed include hash signatures, headers, packers, resources, and metadata [8]. Permission analysis detects abnormal behavior by requesting unusual or using more permissions than set. All Android apps set the allowed permissions in the AndroidManifest.xml file, therefore manifesto file is analyzed for excessive and anomalous permission settings [9]–[11]. Static analysis provides fast detection with low resource usage, but it has the disadvantage that it can be circumvented by methods such as obfuscation or signature changes. In addition, it cannot detect new, unknown malicious apps. Therefore, for effective detection, it must be combined with dynamic analysis.

2) Dynamic Analysis: Also known as a behavioral analysis method, dynamic analysis inspects the app while running using debuggers, decompilers, and disassemblers to analyze the code. This method is slower but better suited to handle obfuscated and encrypted payloads and detect polymorphic and mutated malware [12]. However, it has the disadvantage of being resource intensive. To address this, they use a centralized detection approach that sends the metadata of malicious apps to a cloud analysis server.

Commercial mobile antivirus use a hybrid approach to detect malicious apps, combining static and dynamic analysis. Static analysis can be evaluated by scanning data to determine whether an app is malicious, and dynamic analysis can be evaluated by analyzing behavior through installing and running the target app. Therefore, these characteristics can be used to design mobile antivirus evaluation scenarios and criteria.

B. Antivirus Institution

Existing antivirus test institutions have a long history of testing antivirus, mainly for PCs. They evaluate antivirus products by periodically conducting product tests using their own test environments and evaluation criteria, then certify products that satisfy their evaluation criteria. They publish their test results on their blog and in the media, writing analytical reviews of their tested products. As the security of mobile and IoT devices has become significantly important, these institutions have added a variety of other devices to their tests in recent years. However, the details of the tests and malware samples are not publicly available. Furthermore, most of the products included have significantly higher detection rates than other evaluation studies, causing doubt about the results. We analyzed their published test and evaluation methods and items and adopted them in our experiment design for comparison.

1) AV-TEST [13]: AV-TEST GmbH has been conducting evaluations for Android, Windows, and macOS since 2004 for enterprise, personal, and IoT devices. It periodically evaluates antivirus products using its own AMTSO (Anti-Malware Testing Standards Organization) [14] protocol and scores them in three areas: protection from malicious apps, performance, and usability for users out of 6. It issues a certificate if the total score exceeds 10. The website provides security news, reviews of results, data statistics, and more.

2) AV-comparatives [15]: AV-comparatives periodically evaluates Windows, MacOS, and Android mobile devices and provides free reports and data analyses to the media and public. It conducts detection tests using its collection of legitimate and malicious apps and analyses the results in static and dynamic experiments. AV-comparatives evaluate the performance of apps through mass malware scanning and analyze battery usage to assess the optimization of antivirus then distribute visualized analysis reports to make them easy for the common user to understand.

3) PC Security Labs [16]: Established in 2008, PC Security Labs is an IT consulting agency that analyses and evaluates security products, provides review data, and provides security product consulting suitable for the customer's environment through analyzed products. PC Security Labs is under AMTSO [14] and conducts tests using its experimental protocols to ensure objectivity. It regularly conducts Android mobile antivirus evaluations, collects Android and Apple app data, and collects phishing URLs and spam data to build and provide a security data set.

III. 3. Evaluation criteria design

The previous quality evaluation criteria are unsuitable for assessing commercial mobile antivirus products. Most are designed for security solutions and PC antivirus products, or they only focus on malware detection and limit the overall evaluation of mobile antivirus products. This paper identified common evaluation factors and functions based on various quality evaluation standards and mobile antivirus manuals to enhance the evaluation method for mobile antivirus products. It then established evaluation criteria by simplifying unnecessary evaluation factors. The evaluation criteria were designed with reference to ISO/IEC 25000 [17], ISO/IEC 25010 [18], ISO/IEC 25020 [19], and The Ministry of Science MSIT and ICT of Korea's "Software Technique Evaluation Standards [20]". The evaluation criteria are grouped into five main categories as follows.

1) Functionality, to evaluate performance, such as the accuracy and speed of malicious app detection
2) Resource efficiency, to assess how effectively it uses the mobile device's resources, battery, and whether it causes excessive temperature
3) Usability, to evaluate how user-friendly it is
4) Additional features, to evaluate extra security features like VPN and WiFi security
5) Vendor support, to check for prompt updates and support

A. Experiment Environment Implementation

The experimental environment consists of ten experimental PCs, a server PC on which the commands and databases of experiments are built, and ten mobile devices on which malware is installed and detected. The PCs and mobile devices used for functional and performance analysis are of the same product and OS, and the details are shown in Table I. The mobile devices used in the performance evaluation were selected as low-end devices to easily observe the impact of hardware performance on the evaluation performance. Each mobile device with a mobile antivirus installed was connected to a test PC and configured for centralized control. We developed and used our control software to distribute and install/delete malicious apps simultaneously. Android Debug Bridge commands received from the server are sent to each PC, and the PC sends them to the mobile device to control the experiment. The control PC simultaneously executes the malicious app's download, installation, and deletion commands and saves the status log in the DB in real-time. These procedures established a verification environment suitable for the evaluation criteria so that the same performance test could be performed simultaneously without tester intervention.

B. Malicious App Samples

Financial and security organizations provide malicious apps for performance evaluation and research purposes. Moreover, our crawling system also collects other data. We divided them into six sample groups.

- 1,000 malicious apps collected by malware types, such as phishing, spyware, financial, Trojan, and ransomware
- 10,000 malicious apps from the last three years, selected at random
- 1,000 malicious apps that occurred within the past year
- 5,000 malicious apps related to financial phishing from the last three years
- 100 malicious apps related to financial phishing within three months
- 140 malicious apps within one month

TABLE I
Device specification

PC		Mobile device	
CPU	i5-12400	Device	Samsung Galaxy Tab A7 Lite
Memory	16GB	Memory	32GB
Storage	SSD 500GB	Storage	SD Card 128GB
OS	Windows10 Pro 64bit	OS	Android 13

TABLE II
Overview of selected antivirus

Antivirus	Version
V3 Mobile Security [21]	3.8.0.9
AlyacM [22]	3.0.4.7
ESET Mobile Security [23]	8.2.15.0
Mobile Guard [24]	23.1.2
Avast Mobile Security [25]	23.24.0
Norton 360 [26]	5.76.0.231201002
Avira Antivirus Security [27]	7.22.0
Bitdefender Mobile Security [28]	3.3.224.2368
Kaspersky Standard [29]	11.109.4.11153
Malwarebytes Mobile Security [30]	5.3.4

C. Selection of Evaluation Targets

For the selection of mobile antivirus, we chose popular products that can be downloaded from Google Play, Google's Android application market. Among them, we set three criteria to ensure reliability and compatibility with any kind of device.

1) A product with a high number of downloads on Google Play
2) A reliable product with a rating of 3.5 stars or higher
3) A product that can be installed on various devices, such as tablets

Based on these three criteria, ten products were selected for the experimental environment and are listed in Table II.

D. Experimental Scenario

For the experiment, we collected six malicious app samples and designed the experimental scenarios according to the experimental purpose.

Test 1. Real-time detection of malicious app installations (1,000 malicious apps)
Each malicious app is installed on a mobile device and checked for detection. This experiment is conducted to evaluate the accuracy of dynamic analysis.

Test 2. Manual scan detection of 10,000 malicious apps
The antivirus's manual scan function detects 10,000 malicious apps from the last three years using an external storage device. We use the manual scan feature to evaluate static analysis and experiment with SD cards, assuming that the apps are downloaded from external sources rather than app stores. Moreover, while conducting a manual scan, a large number of malicious apps are scanned to load test the antivirus simultaneously.

Test 3. Detecting 1,000 malicious apps within the last year
We measure detection performance using malicious apps reported within the last year. This test can help determine if the mobile antivirus engine is up to date.

Test 4. Detect 5,000 financial or phishing malicious apps over three years
Measures detection performance specifically for financial and phishing-related malicious apps. This test helps to analyze which products are effective against stealing financial and personal information.

Test 5. Detect 100 financial malicious apps within three months
This test uses manual scanning and install/execution scanning to detect malicious apps collected from financial organizations that have occurred within the last three months. This test uses apps that have caused real-world attacks, allowing us to evaluate the accurate detection performance of antivirus.

Test 6. Detect 140 malicious apps within one month
We test apps that were reported within one month. This allows us to see how quickly manufacturers respond and update their engines.

IV. Experimental Results and Analysis

After completing the preliminary work of developing evaluation criteria, collecting malicious app samples, and building the experimental environment, we conducted the experiments during the month of November 2023. The testing time was limited due to the characteristics of mobile applications, where the detection engine update cycle is faster than antivirus on other platforms. The product names of the ten tested mobile antivirus products are written from A to J.

A. Functionality Evaluation

Functionality evaluation is an accuracy and speed evaluation that checks how quickly and accurately a malicious app is detected when installed on a device or manually scanned for external memory. The results were calculated by testing six experimental scenarios separately and averaging the detection rates, as shown in Figure 2. Accuracy is rated as Good if it detects more than 85% of the apps correctly, Average if it detects more than 75% but less than 85%, and Bad if it detects less than 75%. The number of malicious apps subdivided speed to account for the fact that the scan time increases with the number of malicious apps. For less than 200 malicious apps, the scanning time is Good if it is less than 2 minutes, Average if it is less than 6 minutes, and Bad if it is more than 6 minutes. For more than 1,000 malicious apps, the scanning time is Good if it is less than 10 minutes, Average if it is less than 30 minutes, and Bad if it is more than 30 minutes. As shown in Figure 2, products B and C had the best results, with 10 excellent and one average rating for functionality. Product E could not be tested because it does not support an external storage scan function. The product I was excluded from some evaluations due to problems such as insufficient internal memory during testing.

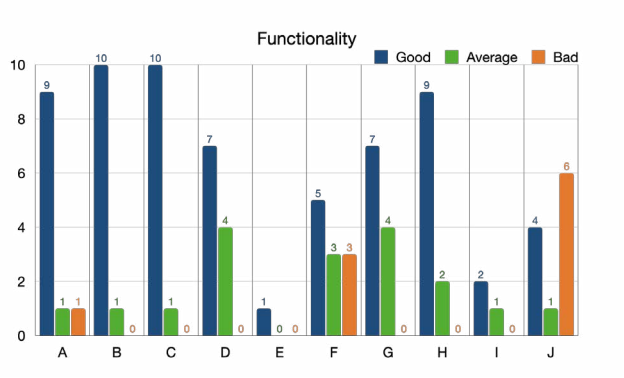

Fig. 2. Functionality analysis result

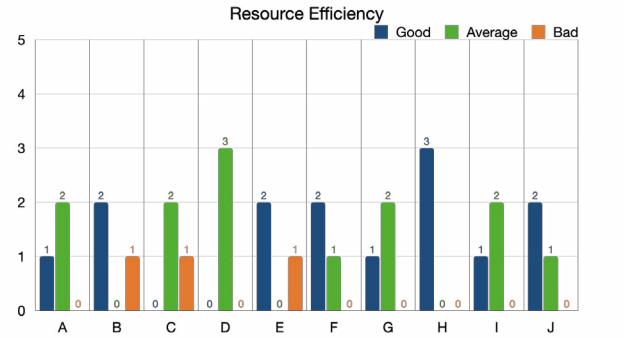

Fig. 3. Resource efficiency analysis result

B. Resource Efficiency Evaluation

Resource efficiency evaluates how much the mobile device's resources consume while scanning for malicious apps. The lower battery consumption and temperature change in this evaluation show better performance. Among the experimental scenarios, it was measured in all experiments except Real-Time Detection. The battery utilization is evaluated by measuring the difference between the battery level before the scan and after scanning 5,000 malicious apps for 3 minutes and the battery level 72 hours after charging the battery to 100% to check the background utilization of the antivirus. For 3 minutes antivirus scan assessment, battery usage is rated as Good if it is less than or equal to 0.3%, Average if it is greater than or equal to 0.3% but less than or equal to 1%, and Bad if it is greater than 1%. For 72 hours Background utilization

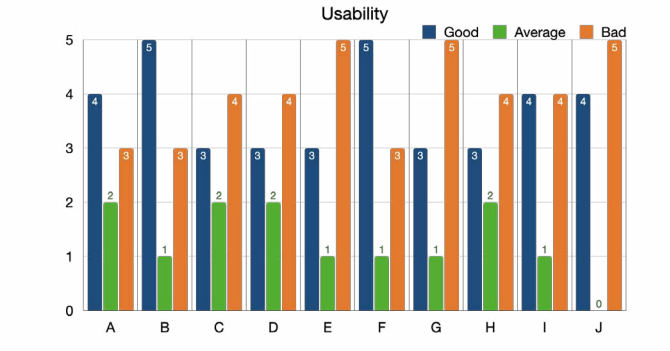

Fig. 4. Usability analysis result

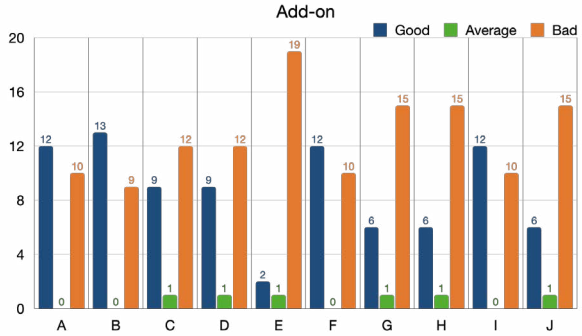

Fig. 5. Add-on functionality analysis result

assessment, battery usage is evaluated as Good if it is less than or equal to 30%, Average if it is greater than or equal to 30% but less than or equal to 50%, and Bad if it is greater than 50%. Temperature was evaluated by checking the temperature change during a 3 minutes antivirus scan of 5,000 malicious apps. If the temperature difference was 2°C or less, it was rated as Good. If it was 4°C or less, it was rated as Average, and if it was more than 4°C, it was rated as Bad ss, as shown in Figure 3. For resource efficiency assessment, product H showed the best results. Among the details, the battery charge rate after 72 hours showed that Product E had a high battery consumption in the background because the battery was discharged.

C. Usability Evaluation

Usability evaluates the ease of use of the product. The ease of user learning is evaluated by how many languages are available and whether the user manual is provided within the product. Input data support evaluates whether the user can specify the desired scan targets for simple and deep scans, and the ease of uninstallation evaluates whether the product can be uninstalled normally without problems. For the items that only ask about support, we rated Good if supported and Bad if not, and for the number of supported devices, we rated Bad if not supported, Average if one or two, and Good if three or more, as shown in Figure 4. There are nine usability subcategories, and Mobile Antivirus B and F have the best results.

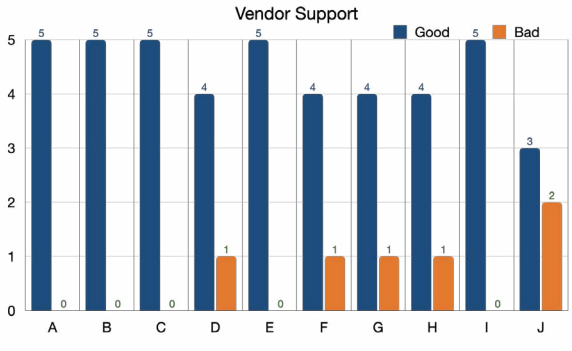

Fig. 6. Vendor support analysis result

D. Add-on Functionality Evaluation

Add-ons functionality are evaluated for providing additional security features. There are 22 detailed evaluation items, including scheduled scans, VPN, WiFi management, and rooting checks. Figure 5 shows the results of the add-on functionality evaluation. Product B has the best results for the add-on functionality evaluation, while Product A offers a variety of manual scanning methods.

E. Vendor Support Evaluation

This evaluation assesses whether features are being added and updated continuously and whether the vendor is responsive in providing support when issues occur. Figure 6 shows the results of the vendor support evaluation. The evaluation results show that items A, B, C, E, and I have excellent results, and relatively all products have good results.

V. Conclusion

The existing quality evaluation criteria and previous studies were simplified and grouped by removing unnecessary items and classified into five main evaluation items: functionality, resource efficiency, usability, additional features, and vendor support. Based on these five categories, 50 detailed evaluation criteria were designed to provide objective and quantitative criteria for evaluating antivirus products targeting mobile devices. We installed ten mobile antivirus products on the devices to validate the evaluation criteria and conducted experiments with static and dynamic analysis types. Then, we validated the evaluation criteria by performing a quality assessment of these products. The results showed that the commercial products performed generally satisfactorily.

Our research team will continue to conduct regular malware detection and long-term usability evaluations with regular testers from the general public. We expect to improve the reliability of our evaluation criteria and enhance our evaluation methodology.

References

[1] P. Taylor, "Mobile subscriptions worldwide 1993-2019," Statista, 06 2023. [Online]. Available: https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993/

[2] J. Lis, "Us time spent with connected devices 2022," EMARKETER, 06 2022. [Online]. Available: https://www.emarketer.com/content/us-time-spent-with-connected-devices-2022
[3] Statista, "Top smartphone users activities 2022," Statista, 07 2023. [Online]. Available: https://www.statista.com/statistics/1337895/top-smartphone-activities/
[4] A. Kivva, "It threat evolution in q1 2024. mobile statistics," Securelist.com, 06 2024. [Online]. Available: https://securelist.com/it-threat-evolution-q1-2024-mobile-statistics/112750/
[5] Zimperium, "2022 global mobile threat report," Zimperium, 2023. [Online]. Available: https://www.zimperium.com/global-mobile-threat-report/
[6] "Android apps on google play," Google.com, 2009. [Online]. Available: https://play.google.com
[7] M. Botacin, F. Ceschin, P. De Geus, and A. Grégio, "We need to talk about antiviruses: challenges & pitfalls of av evaluations," *Computers & Security*, vol. 95, p. 101859, 2020.
[8] J. S. Sraw and K. Kumar, "Using static and dynamic malware features to perform malware ascription," *ECS Transactions*, vol. 107, no. 1, p. 3187, 2022.
[9] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," *IEEE security & privacy*, vol. 7, no. 1, pp. 50–57, 2009.
[10] W. Z. Zarni Aung, "Permission-based android malware detection," *International Journal of Scientific & Technology Research*, vol. 2, no. 3, pp. 228–234, 2013.
[11] D. Barrera, H. G. Kayacik, P. C. Van Oorschot, and A. Somayaji, "A methodology for empirical analysis of permission-based security models and its application to android," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 73–84.
[12] L. Vaishanav, S. Chauhan, S. Kumari, M. S. Sankhla, and R. Kumar, "Behavioural analysis of android malware and detection," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 47, no. 3, 2017.
[13] "Av-test — antivirus & security software & antimalware reviews," AV-TEST. [Online]. Available: https://www.av-test.org
[14] "Amtso - anti-malware testing standards organization," AMTSO. [Online]. Available: https://www.amtso.org
[15] "Av-comparatives," AV-Comparatives. [Online]. Available: https://www.av-comparatives.org
[16] "Pcsl it consulting institute — product testing services, data feeds," PC Security Labs. [Online]. Available: https://www.pitci.com
[17] O. I. de Normalización, *ISO/IEC 25000: Software Engineering-Software Product Quality Requirements and Evaluation (SQuaRE)-Guide to SQuaRE*. ISO, 2005.
[18] I. O. for Standardization, *ISO/IEC 25010: 2011: Systems and Software Engineering-Systems and Software Quality Requirements and Evaluation (SQuaRE)-System and Software Quality Models*. ISO/IEC, 2011.
[19] ——, *ISO/IEC 25020: 2019: Systems and Software Engineering-Systems and Software Quality Requirements and Evaluation (SQuaRE)-Quality measurement framework*. ISO/IEC, 2011.
[20] T. M. o. S. MSIT and I. of Korea, "Software technique evaluation standards," The Ministry of Science and ICT of Korea, 12 2021.
[21] Ahnlab, "Ahnlab mobile security," Ahnlab. [Online]. Available: https://www.ahnlab.com/en/product/mobile-security
[22] ESTsecurity, "Estsecurity corp." ESTsecurity. [Online]. Available: https://en.estsecurity.com/product/alyac_android
[23] ESET, "Antivirus for android with app lock and anti-theft," ESET. [Online]. Available: https://www.eset.com/int/home/mobile-security-android/
[24] S. Shieldus, "Mobile guard," SK Shieldus. [Online]. Available: https://www.skshieldus.com/kor/service/care/adt-caps-mobile.do
[25] Avast, "Free antivirus app for android — avast mobile security," Avast. [Online]. Available: https://www.avast.com/free-mobile-security
[26] Norton, "Norton mobile security for android," Norton. [Online]. Available: https://us.norton.com/products/mobile-security-for-android
[27] Avira, "Avira antivirus security for android," Avira. [Online]. Available: https://www.avira.com/en/free-antivirus-android
[28] Bitdefender, "Bitdefender mobile security for android devices," Bitdefender. [Online]. Available: https://www.bitdefender.com/solutions/mobile-security-android.html
[29] Kaspersky, "Kaspersky standard – powerful antivirus software — kaspersky," Kaspersky. [Online]. Available: https://www.kaspersky.com/standard
[30] Malwarebytes, "Mobile security for android and ios," Malwarebytes. [Online]. Available: https://www.malwarebytes.com/mobile