Recommendation mobile antivirus for Android smartphones based on malware detection

Hendra Saputra[1], Amalia Zahra[2], Faldi[3], Ferry Fadzlul Rahman[4], Sayekti Harits Suryawan[3], Wawan Joko Pranoto[3], Fathur Rahman[1]

[1]Department of Digital Business, Faculty of Science and Technology, Universitas Muhammadiyah Kalimantan Timur, Samarinda, Indonesia
[2]Department of Computer Science, Faculty of Computer Science, Bina Nusantara University, Jakarta, Indonesia
[3]Department of Computer Engineering, Faculty of Science and Technology, Universitas Muhammadiyah Kalimantan Timur, Samarinda Indonesia
[4]Departement of Public Health, Faculty of of Public Health, Universitas Muhammadiyah Kalimantan Timur, Samarinda, Indonesia

Article Info

Article history:

Received Aug 17, 2023
Revised Jan 8, 2024
Accepted Feb 10, 2024

Keywords:

Android malware
Best antivirus
Euphony
Virusshare
Virustotal

ABSTRACT

The proliferation of smartphone malware attacks due to a lack of vigilance in app selection raises serious concerns. Built-in smartphone security features often must be improved to protect devices from these threats. Although numerous articles recommend top-tier antivirus solutions, there need to be more reliable data sources that raise suspicions about undisclosed promotional motives. This research endeavors to establish a ranking of antivirus efficacy to provide optimal recommendations for Android smartphone users. The research methodology entails a meticulous comparison of malware detection and labeling outcomes between various antivirus programs within virustotal and the labeling system employed by the euphony application. The comparative results are categorized into three groups: antivirus solutions proficient in identifying specific malware types, those detecting malware presence without categorization, and antivirus software failing to detect malware effectively. The experimental findings present the five leading antivirus solutions, ranked from the highest to lowest scores, as Ikarus, Fortinet, ESET-NOD32, Avast-Mobile, and SymantecMobileInsight. Based on the comprehensive assessment conducted in this study, these solutions are recommended as the top antivirus choices. These recommendations are poised to significantly aid users in selecting the most suitable antivirus protection for their Android smartphones.

Corresponding Author:

Ferry Fadzlul Rahman
Department of Public Health, Faculty of of Public Health, Universitas Muhammadiyah Kalimantan Timur
Ir. H. Juanda Street No.15, Sidodadi, Samarinda Ulu, Samarinda City, East Kalimantan, 75124, Indonesia
Email: ffr607@umkt.ac.id

1. INTRODUCTION

Currently, the growth in smartphone usage remains remarkably high [1]. Year after year, this growth continues to rise [2]. The current number of smartphones is still predominantly Android-based [3], [4]. Android maintains a dominant position in the mobile operating system market, accounting for approximately 70.79% of the total share[4]. However, the significant number of Android users also attracts the attention of intruders seeking to exploit the negligence of smartphone users, including the creation of Android malware [5]–[8].

Based on the available information on the website, there is evidence of a decrease in the prevalence of Android malware affecting smartphones, suggesting positive developments in addressing security concerns within the Android ecosystem [9]. However, the latest data for the third quarter of 2022 reveals that there are

438,035 malicious packages successfully installed on Android-based smartphones. Despite experiencing a decrease, this figure still shows a significant risk related to malware on the Android platform. This underscores that the security of Android devices remains a crucial issue, and there is a need for more serious attention and preventive measures to protect users from potential security threats.

Companies compete fiercely to develop the best antivirus solutions and promote their products, asserting that their creations can effectively shield devices from Android malware attacks [10]. However, most users still need clarification when selecting the optimal antivirus, given the plethora of choices available in the market [11]. Despite numerous articles on various websites discussing the best antivirus options, users continue to question the authenticity and objectivity of the presented data, as issues of data credibility and objectivity often arise [12]. Certain companies might even pay for favorable product reviews, leading to skepticism among users [13].

This research contributes to developing comprehensive insights into cybersecurity on Android devices. Previous studies have primarily focused on malware attack patterns, the classification of malware families, and the analysis of various malware types [14]–[16]. However, a limit must be placed on determining the best antivirus solutions for Android smartphones. Therefore, this research aims to fill this gap by evaluating and ranking the best antivirus solutions to detect malware on the Android platform effectively. The research approach compares malware detection results from various antivirus programs with the labelling outcomes generated by the Euphony application, providing a more holistic understanding to advance cybersecurity measures on Android devices.

This study aims to narrow its focus by evaluating and ranking the top-performing antivirus solutions designed for detecting malware on the Android platform. The research approach involves comparing the malware detection outcomes of various antivirus programs with the labelling results generated by the Euphony application. In addressing this research gap, the study endeavours to provide a more comprehensive understanding of the effectiveness of antivirus solutions in mitigating the threats posed by malware on Android devices.

2. RELATED WORK

Research related to antivirus performance in malware detection is available in various formats, encompassing academic papers and online articles. Numerous scholarly works delve into the efficacy of antivirus solutions in identifying and mitigating malware threats. In addition to academic literature, online articles contribute valuable insights, presenting a dynamic landscape of discussions and analyses on the evolving challenges and advancements in antivirus technology. Exploring this diverse array of resources enhances the comprehensiveness and depth of understanding in evaluating antivirus performance. Some of these include:

- The study conducted by Thomas aims to prevent devices such as computers, mobile phones, and flash drives from virus attacks. This paper examines the performance of five well-known antivirus software (McAfee, Avast, Avira, Bitdefender, and Norton) on computers. The testing is conducted by analyzing the response time of the antivirus software in quick scans, full scans, and custom scans. Bitdefender demonstrated better performance compared to other antivirus software in addressing malware threats [17].
- The study conducted by IvyPanda discusses the importance of using antivirus software to protect computers from security threats when connected to the internet. Norton and Kaspersky are two well-known antivirus solutions that were analyzed. Norton offers robust protection layers, including Norton Safe Web and parental controls. Kaspersky features real-time protection and network functionalities to combat malware. While Kaspersky performs well in detection, Norton excels with additional features. Overall, both are effective in maintaining computer security against threats [18].
- The research conducted by Christinne involves a comparison of the strengths and weaknesses of 360 security and CM Security as antivirus applications. The aim is to assist smartphone users in selecting an application suitable for their devices. The research methodology encompasses interviews, observations, analysis, and design. The outcomes will be a reference for users to choose the correct antivirus application [19].
- In the article "The Best Antivirus Protection for 2023," an attempt is made to compare the resilience of each computer antivirus in countering malware attacks installed on individual devices. Various testing methods are employed, including firewalls and ransomware protection. The experimental results indicate that Bitdefender and Norton antivirus software outperformed others regarding scores [20].
- The research conducted by Algaith and colleagues yielded empirical analysis results regarding the detection capabilities of 9 AntiVirus (AV) products. These products were tested using 3605 malware samples collected within an experimental network spanning 31 days from November to December 2013. A comparison was made between the detection capabilities of the free AV products available on VirusTotal and the total versions accessible through each vendor's official website. The analysis was based on externally observable attributes of the AV products, specifically whether they could detect specific malware. The research findings reported an in-depth analysis. The striking discovery of this study was that only one vendor's full version could detect all the malware detectable by their VirusTotal version [21].

Overall, the review results indicate that Bitdefender and Kaspersky are antivirus solutions capable of providing robust protection against malware on computer devices. However, the decision to choose the best antivirus still needs to be considered based on users' individual needs and desired features. In safeguarding Android devices, numerous antivirus options offer comparable protection, but selecting one should align with each user's preferences and requirements. Furthermore, validation and direct testing can be critical factors in determining antivirus performance and effectiveness. However, the number of antivirus solutions and samples used may be limited. Research on the best antivirus solutions is predominantly conducted for desktop antivirus applications rather than Android mobile ones.

3. METHOD

Figure 1 illustrates the research flow, beginning with the data collection phase. Data is obtained through extraction using the virustotal application programming interface (API). The API is a conduit for automated access to virustotal's extensive database and services. An API acts as an intermediary that allows different software applications to communicate and exchange information seamlessly. In the context of this research, the virustotal API enables the automated retrieval of information from various antivirus engines related to file analysis and malware detection. Subsequently, the collected data is segmented into two groups: the detection outcome labels from various antivirus solutions and those resulting from the Euphony application process. The next step involves comparing these two data sets to generate a recommendation for the top-performing antivirus solution.

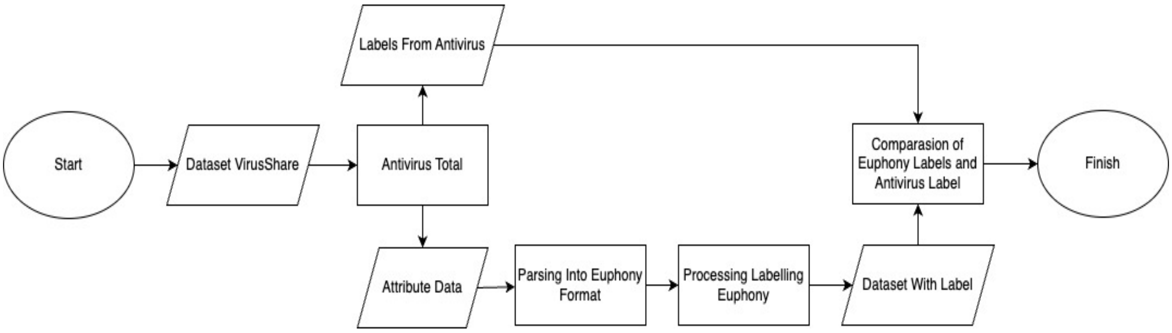
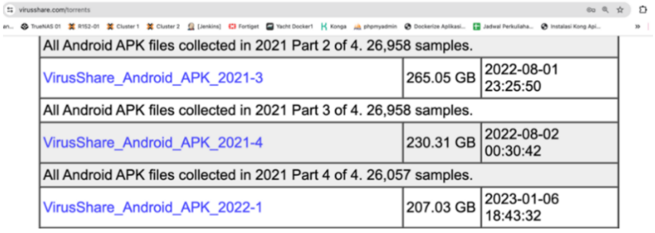

Labels From Antivirus
Start
Dataset VirusShare
Antivirus Total
Comparasion of Euphony Labels and Antivirus Label
Finish
Attribute Data
Parsing Into Euphony Format
Processing Labelling Euphony
Dataset With Label

Figure 1. Research flow

3.1. Data collection

In the initial section, this study will leverage data obtained from the Virusshare website, as illustrated in Figure 2. This repository archives diverse types of malware, including Android malware [22]. VirusShare consistently updates its dataset up to the present time [23]. The Android malware data utilized is extracted from the year 2018, encompassing a total of 28,632 samples. The ample collection of malware from 2018 is a comprehensive reference point for determining the outcomes of the best antivirus calculations.



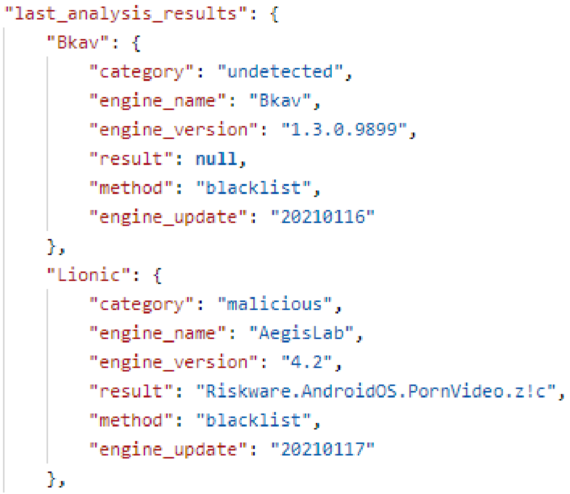
All Android APK files collected in 2021 Part 2 of 4. 26,958 samples.		
VirusShare_Android_APK_2021-3	265.05 GB	2022-08-01 23:25:50
All Android APK files collected in 2021 Part 3 of 4. 26,958 samples.		
VirusShare_Android_APK_2021-4	230.31 GB	2022-08-02 00:30:42
All Android APK files collected in 2021 Part 4 of 4. 26,057 samples.		
VirusShare_Android_APK_2022-1	207.03 GB	2023-01-06 18:43:32

Figure 2. Virusshare from malware android

3.2. Antivirus scanning process from virustotal

The second section will delve into the outcomes of antivirus scanning extracted from the virustotal API. Virustotal is a platform that offers services for analyzing files using over 75 distinct antivirus engines, making it one of the most significant anti-malware scanning systems today [24]. Every uploaded Android malware file to virustotal.com undergoes analysis by numerous antivirus engines. However, not all antivirus solutions can identify a file as malware or assign a specific malware label.

Antivirus scanning results can vary significantly from one antivirus to another, potentially leading to user confusion. The divergent labeling outcomes from different antivirus solutions can perplex users when determining whether a file is indeed malware. To observe the results of uploading Android malware to virustotal.com, please refer to Figure 3. It is essential to emphasize that the introduction of new updates by antivirus vendors may take time to manifest in the scanning results presented on the VirusTotal platform, and this delay could contribute to potential inconsistencies in the reported outcomes [25]. This implies that, in specific instances, the evaluation of an antivirus vendor may not be entirely deemed inaccurate, as the dynamic nature of updates and the varied timelines for their implementation can influence the alignment of the reported scanning results with the latest capabilities of the antivirus solution.



```
"last_analysis_results": {
    "Bkav": {
        "category": "undetected",
        "engine_name": "Bkav",
        "engine_version": "1.3.0.9899",
        "result": null,
        "method": "blacklist",
        "engine_update": "20210116"
    },
    "Lionic": {
        "category": "malicious",
        "engine_name": "AegisLab",
        "engine_version": "4.2",
        "result": "Riskware.AndroidOS.PornVideo.z!c",
        "method": "blacklist",
        "engine_update": "20210117"
    },
```

Figure 3. Results from the virustotal API

3.3. Labeling of malware types from the euphony application

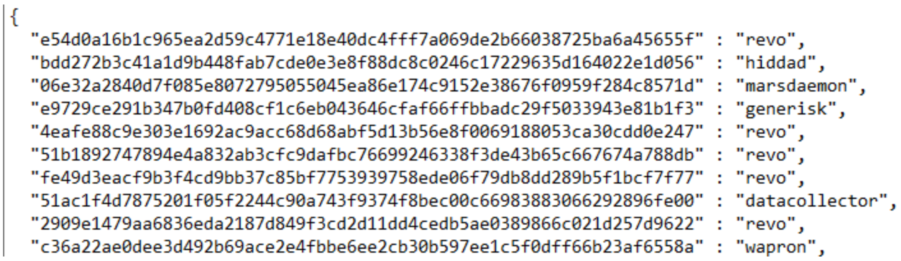
In the third section, we will delve into the comprehensive outcomes derived from the malware-type labelling process orchestrated by the Euphony application. This intricate process is meticulously crafted to assign accurate and informative labels to malware files sourced from VirusShare, initially devoid of any labels. Notably, the diverse labelling of malware samples is a common challenge, as different entities often adopt distinct naming schemes for identical samples. Moreover, the inherent complexity of the labelling process occasionally leads to misclassifications stemming from conceptual errors. The Euphony application will systematically compile scanning outcomes from various antivirus solutions to aggregate a holistic understanding. The Euphony application will aptly determine the appropriate label for each malware file by drawing insights from the most frequently occurring and widely adopted label [26].

Previous studies have demonstrated that the Euphony application can provide labels with high accuracy. Therefore, it is anticipated that this application can offer precise and reliable labeling for previously unlabeled malware files sourced from VirusShare. This labeling outcome holds significance as it will be utilized for comparison with the detection scan results of each antivirus, enabling the assessment of antivirus performance in detecting various types of malware. The results of the malware-type labeling process can be observed in Figure 4.

3.4. Calculation of points for each antivirus

The fourth section will discuss calculating points for antivirus solutions based on the labeling outcomes from the Euphony application. Each antivirus will be evaluated based on the alignment of the labels they provide with the Euphony application's labeling results. If an antivirus assigns the same label as the Euphony application's labeling result, it will be awarded 2 points. This indicates that the antivirus has successfully detected the malware type accurately in accordance with the Euphony application's assessment. If an antivirus assigns a different label from Euphony's labeling result or merely indicates that the file is malware without specifying its type, it will be given 1 point. This point signifies that the antivirus can identify the file as malware but does not align with the label provided by the Euphony application.

Meanwhile, if an antivirus fails to detect malware in each file, it will be assigned 0 points. A score of 0 indicates that the antivirus was unsuccessful in detecting the presence of malware in the tested file. After assigning points to each antivirus scan result, a sorting process is conducted based on the highest points. This aims to generate a list of the best antivirus solutions for detecting Android malware based on their performance. This list will serve as a reference for users to determine the optimal antivirus solution that offers maximum protection for their devices against Android malware threats.



```
{
  "e54d0a16b1c965ea2d59c4771e18e40dc4fff7a069de2b66038725ba6a45655f" : "revo",
  "bdd272b3c41a1d9b448fab7cde0e3e8f88dc8c0246c17229635d164022e1d056" : "hiddad",
  "06e32a2840d7f085e8072795055045ea86e174c9152e38676f0959f284c8571d" : "marsdaemon",
  "e9729ce291b347b0fd408cf1c6eb043646cfaf66ffbbadc29f5033943e81b1f3" : "generisk",
  "4eafe88c9e303e1692ac9acc68d68abf5d13b56e8f0069188053ca30cdd0e247" : "revo",
  "51b1892747894e4a832ab3cfc9dafbc76699246338f3de43b65c667674a788db" : "revo",
  "fe49d3eacf9b3f4cd9bb37c85bf7753939758ede06f79db8dd289b5f1bcf7f77" : "revo",
  "51ac1f4d7875201f05f2244c90a743f9374f8bec00c66983883066292896fe00" : "datacollector",
  "2909e1479aa6836eda2187d849f3cd2d11dd4cedb5ae0389866c021d257d9622" : "revo",
  "c36a22ae0dee3d492b69ace2e4fbbe6ee2cb30b597ee1c5f0dff66b23af6558a" : "wapron",
```

Figure 4. Results of the euphony application's labeling process

4. RESULTS AND DISCUSSION

The findings from our experiments, aimed at identifying the optimal antivirus solution for detecting Android malware through scan result points, are comprehensively presented. This data-rich analysis showcases key metrics such as the total number of scanned files, malware detection based on Euphony labels, discrepancies between malware detection and labels, and the overall malware scanning capability. While the original Table 1 contained extensive data, we have refined our presentation to focus on the top 20 antivirus solutions. This condensed version remains a valuable resource, offering insights into the effectiveness of various antivirus solutions in combating Android malware.

Table 1. Points for each antivirus in detecting android malware

No	Antivirus	Total scan file	Malware detection according to labels	Misaligned malware detection and labels	Inability to detect malware	Point
1	Ikarus	26.718	14.053	9.382	3.283	37.488
2	Fortinet	26.730	11.952	10.570	4.208	34.474
3	ESET-NOD32	26.730	6.642	16.913	3.175	30.197
4	Avast-Mobile	26.730	8.584	12.334	5.812	29.502
5	SymantecMobileInsight	26.730	1.955	23.714	1.061	27.624
6	Avira	26.729	4.911	16.679	5.139	26.501
7	CAT-QuickHeal	26.575	3.084	19.884	3.607	26.052
8	AegisLab	26.727	2.619	19.669	4.439	24.907
9	Microsoft	26.730	3.264	18.104	5.362	24.632
10	K7GW	26.730	0	23.951	2.779	23.951
11	F-Secure	26.723	2.327	18.806	5.590	23.460
12	Alibaba	26.730	3.765	15.714	7.251	23.244
13	Trustlook	26.728	639	21.853	4.236	23.131
14	ZoneAlarm	26.718	2.648	17.398	6.672	22.694
15	Kaspersky	26.724	2.638	17.291	6.795	22.567
16	McAfee	26.730	953	20.649	5.128	22.555
17	NANO-Antivirus	26.729	1.811	18.254	6.664	21.876
18	AhnLab-V3	26.730	490	20.554	5.686	21.534
19	DrWeb	26.730	1.647	18.073	7.010	21.367
20	Symantec	26.728	6	21.104	5.618	21.116

Note:
A=Total scanned files
B=Malware detection according to euphony labels
C=Misaligned malware detection and euphony labels
Calculation of percentages:
Detection according to euphony labels=(B/A)*100
Malware scanning capability=((B+C)/A)*100

The results from Table 1 have successfully ranked the top antivirus solutions in detecting types of Android malware. Based on the comparison between the labelling outcomes from the Euphony application and the scan results of each antivirus, it is evident that numerous antivirus solutions are adept at detecting Android malware effectively. The three top-performing antivirus solutions based on the point calculation are Ikarus Antivirus, Fortinet, and ESET-NOD32, all of which are reputable antivirus providers in the market. Avast-Mobile and SymantecMobileInsight occupy the fourth and fifth positions.

However, 15 antivirus solutions received a score of 0, indicating that these antivirus solutions are entirely incapable of detecting Android malware. This emphasizes that not all antivirus solutions have the same effectiveness level in combating Android malware threats. Users must exercise caution when selecting an appropriate antivirus solution to ensure their devices receive maximum protection against malware attacks. By being informed of the comparison results and rankings of antivirus solutions in Table 1, users can make more informed and intelligent decisions when choosing an antivirus solution that aligns with their needs and device security. In Table 2 results, there is a discrepancy between the percentage of detection according to Euphony labels and the malware scanning capability. Ikarus Antivirus holds the highest percentage in detection according to Euphony labels, while SymantecMobileInsight excels with a 96% malware scanning capability. Both these antivirus solutions stand out as viable choices to be recommended as the best antivirus solutions for Android malware detection.

However, it is crucial to consider the potential for inconsistent data between the information provided by antivirus vendors and the scan results on the VirusTotal platform, which needs to be carefully considered. Nonetheless, the testing and evaluation measures undertaken by antivirus vendors and the results from VirusTotal scans still hold significant value in the effort to safeguard systems against malware threats and potential security risks. Therefore, users are advised to remain proactive in mitigating risks and ensuring system security, including adopting a comprehensive cybersecurity approach.

Table 2. Percentage of the top 5 antivirus solutions

No	Antivirus	Detection according to euphony labels (%)	Malware scanning capability (%)
1	Ikarus	52.6	87.7
2	Fortinet	44.7	84.2
3	ESET-NOD32	24.8	88.1
4	Avast-Mobile	32.1	78.2
5	SymantecMobileInsight	7.3	96

5. CONCLUSION

The conducted experiments have successfully provided recommendations for the best antivirus solutions in Android malware detection. According to Euphony labels, Ikarus Antivirus leads in detection with 52.6%, while SymantecMobileInsight dominates malware scanning at 96%. Both antivirus solutions are well-regarded in the antivirus realm. The results conclude that the top five antivirus solutions possess commendable quality and are worthy protective measures for our smartphones. This is particularly relevant as built-in smartphone security exhibits limitations when facing malware attacks. The derived recommendations offer valuable guidance for smartphone users in selecting antivirus solutions for maximum protection. An antivirus capable of effectively detecting and combating Android malware threats is crucial for maintaining user security and privacy, safeguarding devices from the increasingly complex risks of malware attacks. Relying on the best antivirus solutions gives users greater confidence in using their smartphones without concerns about potential security threats. To ensure more valid research outcomes, further studies are necessary to test the findings, especially regarding the accuracy of Euphony labels, necessitating malware labelling methods with different approaches. Additionally, a more meticulous evaluation of antivirus scan results on VirusTotal is essential, considering that not all antivirus updates are reflected in the "engine update" attribute of the malware scan API. This implies that some antivirus solutions might still need updates, and their capabilities may still need to be fully represented in the scan results. By employing new and more comprehensive approaches, future research is expected to strengthen and complement the findings, providing accurate and reliable results to inform the appropriate use of antivirus solutions in combating Android malware.

REFERENCES

[1] W. Ma, R. Q. Grafton, and A. Renwick, “Smartphone use and income growth in rural China: empirical results and policy implications,” *Electronic Commerce Research*, vol. 20, no. 4, pp. 713–736, 2020, doi: 10.1007/s10660-018-9323-x.

[2] A. Turner, “How many smartphones are in the world?,” *Bank My Cell*, 2022. Accessed: Aug. 15, 2023. [Online]. Available: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.

[3] Y. Zhang *et al.*, “Familial clustering for weakly-labeled android malware using hybrid representation learning,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3401–3414, 2020, doi: 10.1109/TIFS.2019.2947861.

[4] “Mobile operating system market share worldwide,” *Global Statcounter*, 2021. Accessed: Jul. 29, 2023. [Online]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide.

[5] H. Saleous *et al.*, “COVID-19 pandemic and the cyberthreat landscape: research challenges and opportunities,” *Digital Communications and Networks*, vol. 9, no. 1, pp. 211–222, Feb. 2023, doi: 10.1016/j.dcan.2022.06.005.

[6] K. Nomura, D. Chiba, M. Akiyama, and M. Uchida, “Auto-creation of android malware family tree,” *IEEE International Conference on Communications*. IEEE, 2021, doi: 10.1109/ICC42927.2021.9500876.

[7] S. H. Seo, A. Gupta, A. M. Sallam, E. Bertino, and K. Yim, “Detecting mobile malware threats to homeland security through static analysis,” *Journal of Network and Computer Applications*, vol. 38, no. 1, pp. 43–53, 2014, doi: 10.1016/j.jnca.2013.05.008.

[8] A. D. Schmidt *et al.*, “Smartphone malware evolution revisited: android next target?,” *2009 4th International Conference on Malicious and Unwanted Software, MALWARE 2009*. IEEE, pp. 1–7, 2009, doi: 10.1109/MALWARE.2009.5403026.

[9] “Number of detected malicious installation packages on mobile devices worldwide from 4th quarter 2015 to 1st quarter 2021,” *Statista*, 2021. Accessed: Jul. 29, 2023. [Online]. Available: https://www.statista.com/statistics/653680/volume-of-detected-mobile-malware-packages/.

[10] M. L. Yao, M. C. Chuang, and C. C. Hsu, “The kano model analysis of features for mobile security applications,” *Computers and Security*, vol. 78, pp. 336–346, 2018, doi: 10.1016/j.cose.2018.07.008.

[11] S. M. L. D. Lima *et al.*, “Artificial intelligence-based antivirus in order to detect malware preventively,” *Progress in Artificial Intelligence*, vol. 10, no. 1, pp. 1–22, 2021, doi: 10.1007/s13748-020-00220-4.

[12] B. D. Langhe, P. M. Fernbach, and D. R. Lichtenstein, “Navigating by the stars: investigating the actual and perceived validity of online user ratings,” *Journal of Consumer Research*, vol. 42, no. 6, pp. 817–833, 2016, doi: 10.1093/jcr/ucv047.

[13] M. L. Jensen, J. M. Averbeck, Z. Zhang, and K. B. Wright, “Credibility of anonymous online product reviews: a language expectancy perspective,” *Journal of Management Information Systems*, vol. 30, no. 1, pp. 293–324, 2013, doi: 10.2753/mis0742-1222300109.

[14] O. Aslan and A. A. Yilmaz, “A new malware classification framework based on deep learning algorithms,” *IEEE Access*, vol. 9, pp. 87936–87951, 2021, doi: 10.1109/ACCESS.2021.3089586.

[15] C. Ding, N. Luktarhan, B. Lu, and W. Zhang, “A hybrid analysis-based approach to android malware family classification,” *Entropy*, vol. 23, no. 8, p. 1009, Aug. 2021, doi: 10.3390/e23081009.

[16] R. B. Hadiprakoso, H. Kabetta, and I. K. S. Buana, “Hybrid-based malware analysis for effective and efficiency android malware detection,” *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*. IEEE, pp. 8–12, 2020, doi: 10.1109/ICIMCIS51567.2020.9354315.

[17] R. Thomas and M. Nachamai, “Performance investigation of antivirus - a comparative analysis,” *Oriental journal of computer science and technology*, vol. 10, no. 1, pp. 201–206, 2017, doi: 10.13005/ojcst/10.01.27.

[18] “Comparison a norton and kaspersky antivirus software research paper,” *IvyPanda*, 2019. Accessed: Aug 10, 2023. [Online]. Available: https://ivypanda.com/essays/security-products-research-paper/.

[19] M. E. L. S. Y. R. S. Christinne M. T. P. Subagyo, “Comparative study of antivirus adoption rates on smartphone-based operating systems,” *International Journal of Information Technolgy and Education*, vol. 1, no. 1, pp. 108–115, 2021.

[20] N. J. Rubenking, “The best android antivirus for 2023,” *PCMag*, 2023. Accessed: Jul. 30, 2023. [Online]. Available: https://www.pcmag.com/picks/the-best-android-antivirus-apps.

[21] A. Algaith, I. Gashi, B. Sobesto, M. Cukier, S. Haxhijaha, and G. Bajrami, “Comparing detection capabilities of Antivirus products: an empirical study with different versions of products from the same vendors,” *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2016*. IEEE, pp. 48–53, 2016, doi: 10.1109/DSN-W.2016.45.

[22] “About VirusShare.Com,” *Virus Share*, 2023. Accessed: Aug 20, 2023. [Online]. Available: https://virusshare.com/about.

[23] V. Kouliaridis, G. Kambourakis, and T. Peng, “Feature importance in android malware detection,” *Proceedings-2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*. IEEE, pp. 1449–1454, 2020, doi: 10.1109/TrustCom50675.2020.00195.

[24] S. Zhu, Z. Zhang, L. Yang, L. Song, and G. Wang, “Benchmarking label dynamics of VirusTotal engines,” *Proceedings of the ACM Conference on Computer and Communications Security*. ACM, pp. 2081–2083, 2020, doi: 10.1145/3372297.3420013.

[25] P. Peng, L. Yang, L. Song, and G. Wang, “Opening the blackbox of virustotal: analyzing online phishing scan engines,” *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*. ACM, pp. 478–485, 2019, doi: 10.1145/3355369.3355585.

[26] M. Hurier *et al.*, “Euphony: harmonious unification of cacophonous anti-virus vendor labels for android malware,” *IEEE International Working Conference on Mining Software Repositories*. IEEE, pp. 425–435, 2017, doi: 10.1109/MSR.2017.57.

BIOGRAPHIES OF AUTHORS

Hendra Saputra is a lecturer in the Informatic Engineering program at Muhammadiyah University of East Kalimantan, Indonesia. He earned a bachelor’s degree in Informatic Engineering from Muhammadiyah University of Malang in 2017, and a Master's degree in Informatics Engineering from Binus University in 2021. His IT career started at the Information Technology unit of UMKT in 2017. His research focuses on the fields of network and server infrastructure, information systems, and machine learning. He can be contacted at email: hs048@umkt.ac.id.

Amalia Zahra is a lecturer at the Master of Information Technology, Bina Nusantara University, Indonesia. She received her bachelor’s degree in computer science from the Faculty of Computer Science, University of Indonesia (UI) in 2008. She does not have a master’s degree. Her Ph.D. was obtained from the School of Computer Science and Informatics, University College Dublin (UCD), Ireland in 2014. Her research interests cover various fields in speech technology, such as speech recognition, spoken language identification, speaker verification, speech emotion recognition, and so on. Additionally, she also has interest in natural language processing (NLP), computational linguistics, machine learning, and artificial intelligence. She can be contacted at email: amalia.zahra@binus.edu.

Faldi is a lecturer in the field of Computer Science at Universitas Muhammadiyah Kalimantan Timur. With an educational background of a Bachelor's degree in Computer Science from STIMIK Widya Cipta Dharma and a Master's degree in Information Technology from Binus University. He possesses a strong knowledge in the field of computer science and artificial intelligence (AI). As a professional with expertise in networking. He has the ability to design, manage, and solve complex networking issues. On the other hand, his proficiency in artificial intelligence enables him to develop innovative AI solutions, such as machine learning models and practical computer vision applications. He can be contacted at email: fal146@umkt.ac.id.

Ferry Fadzlul Rahman is a lecturer in the field of Public Health at Universitas Muhammadiyah Kalimantan Timur. He holds a doctoral degree from Asia University, Taiwan. With a strong educational background and expertise in artificial intelligence (AI) in healthcare. He brings valuable knowledge to his role. His proficiency in application health programe. He can be contacted at email: ffr607@umkt.ac.id.

Sayekti Harits Suryawan is a lecturer in the field of Computer Science at Universitas Muhammadiyah Kalimantan Timur. He holds a bachelor's degree (S.Kom.) from Universitas Mulawarman and a master's degree (M.Kom.) from Institut Teknologi Sepuluh Nopember. With a strong educational background in Computer Science and Artificial Intelligence (AI), Sayekti possesses extensive knowledge in networking and AI. He has the ability to design, manage, and solve complex networking issues, as well as develop innovative AI solutions, such as machine learning models and practical computer vision applications. He can be contacted at email: shs500@umkt.ac.id.

Wawan Joko Pranoto is a lecturer in the field of Public Health at Universitas Muhammadiyah Kalimantan Timur. He holds a bachelor's degree (S.Kom.) from STMIK Samarinda, a master's degree (M.T.I.) from Universitas Bina Nusantara, and a doctoral degree from Asia University, Taiwan. With a strong educational background and expertise in artificial intelligence (AI) in healthcare. He brings valuable knowledge to his role. His proficiency in application health programs is notable. He can be contacted at email: wjp337@umkt.ac.id.

Fatur Rahman is currently studying in the Digital Business program. He is focused on gaining comprehensive knowledge and skills in the field of digital business, including e-commerce, digital marketing, and business analytics. His studies are aimed at equipping him with the tools and expertise needed to excel in the rapidly evolving digital business landscape. He can be contacted at email: 2211102453002@umkt.ac.id.