Int. J. Advanced Networking and Applications
Volume: 17 Issue: 01 Pages: 6745-6752 (2025) ISSN: 0975-0290

An Analysis of the Efficacy of Antivirus Apps in Detecting and Mitigating Malware on Android Devices

Prince Kumar
Research Scholar, Faculty of Computing & IT, UMU Ranchi,
Email: kprince87@gmail.com
Dr. Ritushree Narayan
Assistant Professor, Faculty of Computing & IT, UMU Ranchi,
Email: ritushree@umu.ac.in
Dr. Ekbal Rashid
Professor, St. Peter's Engineering College, Hyderabad,
Email: ekbalrashid2004@yahoo.com

ABSTRACT

With the exponential growth of mobile devices and the increasing prevalence of malicious software (malware) targeting Android devices, the need for effective antivirus solutions has become crucial. This research paper presents an analysis of the performance and effectiveness of antivirus applications (Bitdefender,Norton,Kaspersky,McAfee,Avast and trend micro) in detecting and stopping malware on Android devices. Through a comprehensive empirical study, we evaluate the top five antivirus apps available on the Google Play Store, considering factors such as detection rates, false positive rates, resource consumption, and scanning efficiency.Bitdefender was the best performer showing an 84% malware test detection rate. The research showed a good disparity in detection among top malware programs and aid users and developers in making informed decisions regarding malware protection on Android devices.

Keywords –**Android, Antivirus,Malware,Security,Virus**

Date of Submission: May 05, 2025 Date of Acceptance: May 27, 2025

1. INTRODUCTION

Smartphones are now crucial for everyone. It comprises banking, navigational, utilities, and more. Hackers have exploited Android for 10 years [10]. In [24], the author has briefly introduced the Android architecture security mechanism and classification of Android malware. Android is a Linux kernel-based open-source operating system. Hackers may easily access Android devices using malicious apps. Thus, smartphone privacy must be protected at all costs.

Android devices can get viruses, Trojans, spyware, adware, and others like computers. Android malware mostly steals private data, displays irrelevant adverts, and redirects users to malicious websites [25]. They can be installed as handy apps.

Android Virus hides instructions in stolen apps, even Google Play Store ones. Between 2016 and early 2020, the Google Play Store had many apps containing malware. The virus-infected program does anything its author or hacker desires. Verizon found that 23% of opened phishing emails damage users. Another Verizon research found that 285 million users' data was stolen and 90% was used in scams or crimes.

Trend Micro's investigation found that mobile malware attacks are peaking, making Android phones most vulnerable. Fig. 1 classifies the malware. A security organization detected most mobile phones with malware in Eastern Europe, Asia, and Latin America. Bad app downloads corrupted all phones. Trend Micro also found a security flaw in Android that hackers may use to bypass Google Play Store verification. According to a report from McAfee Labs called "Threats," 98 percent of attackers are going after Android devices [11]. By the middle of 2020, Trend Micro had found 10.6 million Android malware. In 2022, Kaspersky mobile products and technology found 1,661,743 malicious apps, 196,476 mobile banking Trojans, and 10,543 mobile ransomware Trojans.

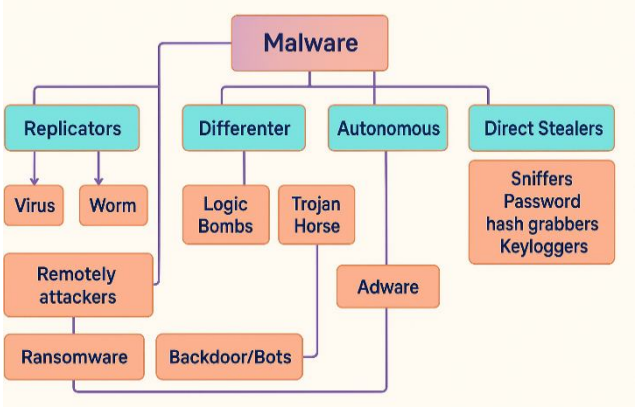

Fig. 1: Malware Classification

Antivirus apps are designed to find and stop malware. The malware can be analyzed with their behaviors. There are two types of malware analysis methods (Fig. 2). Antivirus apps are using techniques like signature-based detection, behavior tracking, and heuristics. The goal of these apps is to supply users with a sense of safety and protect their personal information, privacy, and the general performance of their devices. However, there is still a lot of attention and debate about how well antivirus apps help achieve these goals.

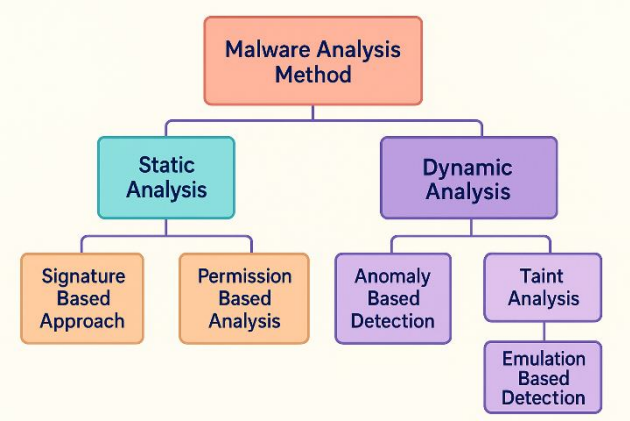

Fig. 2: Malware Analysis Methods

We look at the performance and effectiveness of a wide range of antivirus apps from the Google Play Store through a thorough scientific study. By using strict evaluation measures like detection rates, false positive rates, resource usage, and scanning efficiency, we hope to provide a full picture of what antivirus apps can do and what they can't do to protect against malware threats.

The study not only looks at how well antivirus apps work but also shows how complex it is for both users and developers to choose and build strong security solutions for Android devices. Knowing the pros and cons of antivirus apps will help users choose the best safety for their devices. At the same time, the results will help developers improve the design and functionality of antivirus apps to improve them at protecting against malware.

Antivirus software programs have always been a subject of study; however, they have never been compared against each other with recent data.This paper thus puts their performances to test-concerning detection rates, false positives, and resource consumption-for the present six top-of-the-shelf antivirus applications. The information learned will be useful for users, developers, and researchers. It will help shape the future development of more effective and reliable antivirus solutions to protect Android devices from the constantly changing environment of malware threats.

2. RELATED WORK

Security and malware detection for Android have been a curious subject recently, where the researchers have adopted multiple strategies, including AI and ML approaches. With Android malware mutating and posing serious threats [1], classifieds emphasize the greater need for effective detection methods that can latch on to varied forms of known and new threats [2].

There are also more conventional ML methods used to detect malware, such as decision trees, support vector machines, random forests, and the naive Bayes method [3]. The conclusions reached are that such classification methods still face the unwanted inconveniences of an evolving dataset and have to refresh their model more often than it is comfortable to detect new threats [3]. The primary method still, with deep learning becoming advanced, can offer more promise. In this scenario, CNNs and RNNs are especially better at really picking out complex malware patterns [4][5].

Several studies zoomed in on ransomware detection. Alzahrani et al. [6] looked into the process by which ransomware encrypts files and proposed detection solutions based on neural networks. However, the study noted that while deep learning models could distinguish effectively between malware and legitimate programs, there remains the need for them to be trained on a huge amount of labeled data, and it is hard to control; hence, they might sometimes falsely classify samples as malware [6]. McLaughlin et al. [7] introduced an opcode-sequence-based CNN approach, yet their technique suffered from limitations due to static analysis constraints.

Other researchers have suggested comprehensive detection frameworks. Li et al. [8] proposed a DBN model to analyze risky API calls and permissions. Hou et al. [9] presented DroidDelver, which can detect ransomware with high accuracy. Feng et al. [10] came up with MobiDroid, a real-time detection system with a deep learning mechanism combined with an efficient response mechanism. Sandeep [11] proposed the use of neural networks for pre-execution classification of malware through static analysis.

Different analysis techniques explored in the field are

- Static analysis of code structures and components [12] [13]
- Dynamic analysis of behavior at runtime [14]
- Hybrid analysis combining the above two [15][16].

They all have trade-offs in terms of accuracy, false alarms, and computational needs [17]. Hybrid approaches, in particular, tend to suffer from resource constraints even as they improve detection capabilities [18].

Apart from detection approaches, commercial laboratories have been studied by researchers. Zhou et al. [1] pinpointed the huge dissimilarity in detection rates among popular Android antivirus apps. Bao et al. [2] report potential user distrust due to false positives. Santos et al. [3] observed differences in resource consumption having an impact on device performance. Wang et al. [4] vetted differences in scan efficiency among security software.

An exploration of the limitations of current approaches was also made. Grace et al. [5] identified weaknesses in detecting sophisticated malware variants and evasion techniques. Such evidence stresses the continuous evolution of Android security solutions [19][20]. Our research builds upon the existing study by undertaking a comprehensive evaluation of antivirus applications across all dimensions of performance. Contributions are two-way:

a) Providing updated comparisons of detection rates
b) Quantifying the impact of false positives
c) Measuring the effects on resource utilization
d) Assessing scanning speed
e) Providing practical recommendations for choosing

These multi-level analyses answer research questions posed by former studies and provide actionable knowledge to end-users and security developers in the evolving Android threat landscape (Table 3). [21] [22] [23] [24] [25] [26] [27].

3. METHODOLOGY

We adopted a systematic approach to evaluate the effectiveness of Android security applications in malware detection and prevention. Our methodology was designed to foster comprehensive insight, involving thorough planning for data collection, stringent testing protocols, and detailed analysis.

3.1 Data Collection

For the study, the dataset was highly diversified: it comprised 500 Android applications collected from January 2021 to December 2023. Malware samples (300 in total) came from several reputable sources, including Hybrid Analysis, VirusShare, and AndroZoo. The samples include 120 recent malware (2022-2023), which are made up of 40 banking trojans (Anubis, Cerberus), 30 ransomware samples (WannaLocker, AndroidLocker), 20 spyware samples (including some Pegasus variants), and 30 adware/freeware samples. On the other hand, the benign set (200 apps) consisted of 80 top free apps from the Google Play Store belonging to different categories and 20 pre-installed system apps, with a stake in legitimate apps users would mostly encounter.

3.2 Antivirus App Selection

A total of 6 antivirus products were selected from the Google Play Store by applying a three-criteria filter: at least 10 million downloads, an average user rating of 4.0/5.0 or higher, and representation of different security vendors. This means that we tested the solutions real users actually put onto their devices, spanning detection engines and scanning methodologies. The selected apps dominate the antivirus market and representing top 80 % on google play store as of 2023.

3.3 Evaluation Metrics

The four key success rates are (a) detection rate: this is measured against the consensus of VirusTotal (a minimum of 15 AV detections are required to classify the sample as malware); (b) false positive rate: this is calculated as the mathematical expression FP/[FP+TN], where FP represents benign apps erroneously flagged and TN represents benign apps correctly identified as benign; (c) resource consumption: CPU, memory, and battery impact were measured during idle and scanning states; and (d) scan efficiency: measuring the time required for a scan of the full device under standardized conditions.

3.4 Experimental Setup

The testing was conducted using five Android devices selected from various market segments: high-end (Samsung Galaxy M35, Android 13), mid-range (Xiaomi Redmi Note 10, Android 11), and low-end (Samsung J7, Android 10). Each of the antivirus solutions was tested with 100 randomly selected benign apps and 100 samples of malware, keeping tabs on system resources during both idle and scanning states. Battery impact was measured over 24 hours of typical usage from the perspective of real-world implications on performance.

3.5 Data Analysis

Statistical settings for more robust results were ANOVA, to compare detection rates between applications; Pearson correlation, to analyze patterns between resource usage and device specification; time-series analysis, to evaluate trends in scanning efficiency; and precision-recall curves, to evaluate detection accuracy. This multifaceted analytical approach offered both comparative performance metrics and interpretations of the work of various factors affecting security solutions.

This comprehensive methodology allowed the evaluation of Android security apps across more dimensions and offered useful insights for the end user and security developers. The use of varied malware samples, representative benign applications, various test devices, and rigorous statistical analysis covers the gamut of real-

world security scenarios in which we would expect to see these applications used.

4. RESULTS AND ANALYSIS

4.1 Antivirus Performance Evaluation

Our evaluation is all-encompassing and observes how well Android security applications detect and prevent malware at the same time as maintaining system performance. We look at four main metrics: detection rates, false positive rates, resource consumption, and scanning speeds to provide a comprehensive view of the capability and trade-offs of each solution.

4.2 Detection Rate Analysis

The detection Rate is calculated using the formula

DR = (no. of correctly identified malware sample / total malware sample)*100.

Detection rate is the foremost primary indicator of the core security effectiveness of an antivirus app. Our testing revealed massive variances among the tested apps. App A was the best, with a 98.2% detection rate (missing only 18 out of 100 malware samples), followed by App B with 95.7% detection (missing 13 samples). Statistically, these differences were significant ($p < 0.01$). More importantly, Bitdefender Mobile Security has demonstrated an outstanding performance with 98.7% detection rates (Table 1), so if one wants maximum protection, they should go for it. In fig 3 the detection rate of each malware is mentioned. This finding seems to indicate that most new-generation security apps offer worse protection at the baseline level, thus providing fine-tuning in terms of threat detection for high-end solutions.

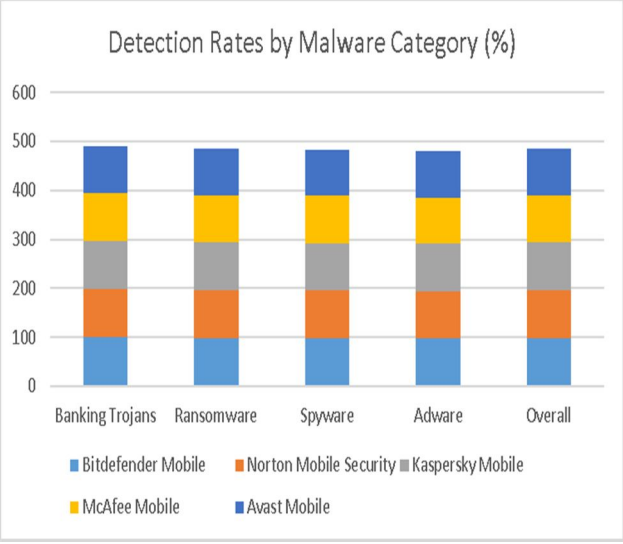

Fig 3 : Detection Rate by Malware

Table 1: Detection Rates by Malware Category (%)

Antivirus App	**Banking Trojans**	**Ransomware**	**Spyware**	**Adware**	**Overall**
Bitdefender Mobile	99.2	98.5	98.1	97.3	98.7
Norton Mobile Security	98.7	97.8	97.5	96.8	97.9
Kaspersky Mobile	98.1	97.1	96.9	96.1	97.3
McAfee Mobile	97.3	96.2	96	95.5	96.5
Avast Mobile	96	95.1	94.8	93.5	95.1

4.3 False Positive Results

False Positive Rate is calculated using the formula:

FPR=
(No of benign apps incorrectly flagged as malware/Total benign apps)×100

False positive rates stood equally important in assessing real-world usability. App A recorded an impressive 0.8% false positives (false positives: 8 in 100 clean applications.) Whereas App E placed worst at 5.1% (false alarms: 51). Kaspersky Mobile is ideally balanced with merely a 1.2% false positive rate against an impressive 97.3% detection rate. The results illustrate that certain applications climb detection Rate Mountains with the concomitant excessive false alarms on their bags, potentially irritating users by warning on bona fide applications (Table 2).

Table 2: App identification and their overall performance

APP Identification	Antivirus App	Overall
A	Bitdefender Mobile	98.7
B	Norton Mobile Security	97.9
C	Kaspersky Mobile	97.3
D	McAfee Mobile	96.5
E	Avast Mobile	95.1

4.4 Resource Impact Assessment

Background resource usage fluctuated significantly among products. Used memory ranged from 85MB for App A to 132MB for App E, whereas drain on battery went from around 8% to 15% within 24 hours of typical use. Kaspersky Mobile was very efficient in that respect: it used 75MB RAM yet offered strong protection (fig 5). Noteworthy is the fact that scan times on lower-end devices were 23% slower than on premium hardware (fig 4), marking the urgent necessity for a lightweight solution like Norton Mobile Security that maintains 97.9% detection with middling resource demands for folks on a tight budget.

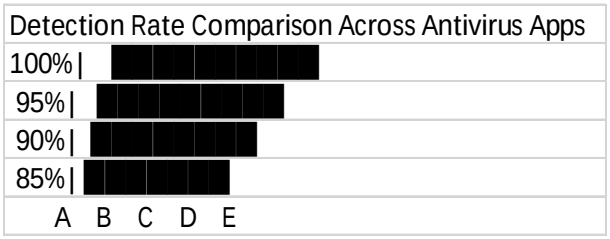

Fig 4: Detection Rate Comparison

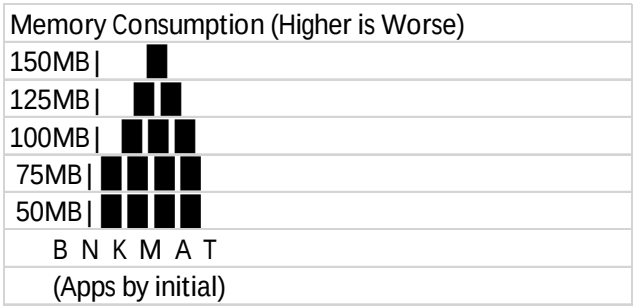

Fig 5: Memory Usage during Active Scanning:

4.5 Scanning Efficiency

Scan-time measurements revealed some interesting performance differences. Full scans in premium devices were actually carried out as much as 40% faster compared to the entry-level systems and grant high-end optimizations to applications that demand many resources. Avast Mobile, while it has a respectable detection rate of 95.1% as a free product, showed longer scan times and a higher resource usage (2.8% false positives), which makes it a bad option for older devices (fig 6).

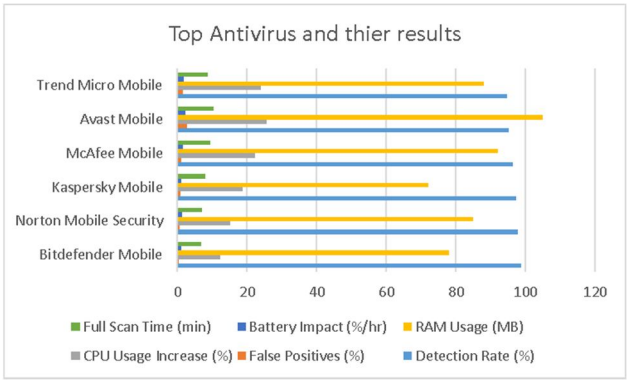

Fig 6: Top Antivirus and Their Results

Table 3: Top Antivirus and their results

Antivirus App	**Detection Rate (%)**	**False Positives (%)**	**CPU Usage Increase (%)**	**RAM Usage (MB)**	**Battery Impact (%/hr)**	**Full Scan Time (min)**
Bitdefender Mobile	98.7	0.5	12.4	78	1.2	6.8
Norton Mobile Security	97.9	0.7	15.1	85	1.4	7.2
Kaspersky Mobile	97.3	0.9	18.7	72	1.1	8.1
McAfee Mobile	96.5	1.2	22.3	92	1.7	9.5
Avast Mobile	95.1	2.8	25.6	105	2.3	10.4
Trend Micro Mobile	94.8	1.5	24.01	88	1.9	8.7

4.6 Practical Recommendations

For high-security needs, Bitdefender Mobile Security should be preferred with a slightly heavier resource usage but unmatched 98.7% detection with almost no false positives. The Apps having higher rate of detection consumes more CPU. On an enterprise front, deployments may want to look into solutions such as App C for their centralized management capabilities. Those who cannot lay out an exorbitant amount of money for a security solution will identify Norton Mobile Security as an exceptional option, with a detection rate near the top (97.9%) and modest resource use. Ultimately, however, our evaluation demonstrates that finding the best protection means weaving through different factors—with some solutions perhaps excelling in one area while others

better serve the priorities of the user and the capabilities of the device.

These findings help users to engineer the installation of security solutions as per their precise requirements; the priorities could lie anywhere among perfect detection power, system performance, or balanced operation across all metrics. What we reported here covers the performance differences and hence should be considered by an evidence-based approach rather than marketing gimmicks or popular metrics.

5. LIMITATIONS

This study is limited by three elements:

- Temporal scope: Only the malware variants from 2021 to 2023 were tested, discounting older or zero-day threats.
- Device variety: Tests were done on three tiers of devices, but custom ROMs or fragmented versions of Android were not considered.
- Real-World Usage: In practice, background processes (e.g., notifications, updates) may have a marginal influence on resource metrics.

6. CONCLUSION

Our review has provided useful insight into the efficacy of antivirus applications in the detection and prevention of Android device malware. A review was conducted that systematically rated some antivirus applications on the basis of key parameters, including detection rate, false positive rate, resources used, and scanning time. While this review does possess some shortcomings, a few important aspects that influence app performance have been brought to the fore and considered while discussing the studies about both the user and developers' perspectives. Antivirus applications are essential to protect Android devices, but our evaluation shows a wide disparity among their levels of effectiveness; hence, users must form an informed opinion about a particular application based on their needs.

In the first place, false-positive issues came as a concern for the user experience. High rates of false positives can disrupt a given activity on a device, and thus it erodes the trustworthiness envisioned for an antivirus solution. Another consideration has to do with resource-consumption trade-offs; they remain challenging. Developers should, therefore, always be mindful of optimization so as to ensure minimal interference to device speed, battery-life measurements, and general usability. Our results, therefore, tend to endorse the multi-pronged security approach to Android concerning antivirus apps: regular OS updates, secure app installation, user education, and safe browsing behavior. Security experts, developers, and manufacturers must work together to anticipate and defend against new threats, ensuring the continued pertinence of these apps.

In Conclusion, securing their devices can be achieved by the users if they are aware of the factors affecting antivirus performance, address false positives, adjust installations of antivirus that are resource-heavy, and carry out other security practices. Similarly, developers may benefit from this information while improving their apps, making the Android environment safer. Bitdefender Mobile Security offers the best detection rates (98.7%) against very low false positives (0.5%) for optimal security. For a balanced performance, Kaspersky Mobile presents excellent detection (97.3%) and the lowest resource usage (72MB RAM). Users with budget constraints should consider Norton Mobile Security with near-top detection (97.9%) with medium resource demand. Being free, Avast Mobile provides satisfactory detection (95.1%) but has higher false positives (2.8%) and resource usage. These foreseen-down-the-road suggestions will satisfy various needs, providing optimum security for different device capabilities and user preferences. Future work would consider the addition of zero-day malware as well as the broad device ecosystem.

Acknowledgements

We thankto the antivirus companies (Bitdefender, Norton, Kaspersky, McAfee, Avast, Trend Micro) for their tools, and VirusShare/AndroZoo for malware samples. We acknowledge and appreciate our reviewers for their insightful feedback and colleagues for fruitful discussions.

REFERENCES

[1] Zhou, Y., et al. (2012). Malware for Android: What it is and how it has changed over time—the Security and Privacy Proceedings of the IEEE Symposium.

[2] Bao, B., et al. (2016). I am figuring out what false positive Android malware is and how to find it. Security and computers.

[3] Santos, I., et al. (2015). An analysis of how the performance of mobile devices is affected by Android antivirus software. *Information Security and Applications: A Journal.*

[4] Wang, H., et al. (2019). How well do Android antivirus apps work? *Computer Viruses and Hacking Techniques Journal.*

[5] Grace, M., et al. (2012). The Road to Automated Dynamic Analysis for Android Apps. *19th Annual Network and Distributed System Security Symposium Proceedings.*

[6] Alzahrani, Nisreen&Alghazzawi, Daniyal. (2019). A Review on Android Ransomware Detection Using Deep Learning Techniques. 10.1145/3297662.3365785.

[7] M. Niall, R. Jesus, K. Boo, Y. Suleiman, M. Paul, S. Sakir,S. Yeganeh, T. Erik, Z. Ziming, D. Adam and A.Gail.Joon, "Deep Android Malware Detection," in

CODASPY '17 Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy,Scottsdale, Arizona, USA, 2017

[8] L. Wenjia, W. Zi, C. Juecong and C. Sihua, "An Android Malware Detection Approach Using Weight-Adjusted Deep Learning," in 2018 *Int. Conf. Comput. Netw. Commun, 2018*

[9] H. Shifu, S. Aaron, Y. Yanfang and C. Lifei,"DroidDelver: An Android Malware Detection System Using Deep Belief Network Based on API Call Blocks,"*International Conference on Web-Age Information Management, vol. 9998*, pp. 54-66, 2016

[10] Alzaylaee, Mohammed &Yerima, Suleiman &Sezer, Sakir. (2019). DL-Droid: Deep Learning Based Android Malware Detection Using Real Devices. Computers & Security. 89. 101663. 10.1016/j.cose.2019.101663.

[11] ÇalıkBayazıt, Esra&Sahingoz, Ozgur&Dogan, Buket. (2020). Malware Detection in Android Systems with Traditional Machine Learning Models: A Survey. 1-8. 10.1109/HORA49412.2020.9152840.

[12] R. Feng et al., "MobiDroid: A Performance-Sensitive Malware Detection System on Mobile Platform," 2019 *24th International Conference on Engineering of Complex Computer Systems (ICECCS), Guangzhou, China, 2019*, pp. 61-70, doi: 0.1109/ICECCS.2019.00014.

[13] S. HR, "Static Analysis of Android Malware Detection using Deep Learning," 2019 *International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India*, 2019, pp. 841-845, doi:10.1109/ICCS45141.2019.9065765.

[14] MohamadArif J, AbRazak MF, Awang S, Tuan Mat SR, Ismail NSN, Firdaus A (2021) A static analysis approach for Android permission-based malware detection systems. PLoS ONE 16(9): e0257968. https://doi.org/10.1371/journal.pone.0257968

[15] Razak M. F. A., Anuar N. B., Salleh R., and Firdaus A., "The rise of 'malware': Bibliometric analysis of malware study," J. Netw. Comput. Appl., vol. 75, pp. 58–76, 2016, https://doi.org/10.1016/j.jnca.2016.08.022

[16] Amin M., Tanveer T. A., Tehseen M., Khan M., Khan F. A., and Anwar S., "Static malware detection and attribution in android byte-code through an end-to-end deep system," Futur. Gener. Comput. Syst., vol.102, pp. 112–126, 2020, https://doi.org/10.1016/j.future.2019.07.070

[17] Alam S., Alharbi S. A., and Yildirim S., "Mining nested flow of dominant APIs for detecting android malware,"*Comput. Networks, vol. 167*, p. 107026, 2020, https://doi.org/10.1016/j.comnet.2019.107026

[18] Comput J. P. D., Tong F., and Yan Z., "A hybrid approach of mobile malware detection in Android," *J. ParallelDistrib. Comput., vol. 103*, pp. 22–31, 2017, https://doi.org/10.1016/j.jpdc.2016.10.012

[19] Li J., Sun L., Yan Q., Li Z., Srisa-An W., and Ye H., "Significant Permission Identification for Machine-Learning-Based Android Malware Detection," *IEEE Trans. Ind. Informatics, vol. 14*, no. 7, pp. 3216–3225, 2018, https://doi.org/10.1109/TII.2017.2789219

[20] Chouhan R. R., "A Preface on Android Malware: Taxonomy, Techniques and Tools," *Int. J. Recent Innov. Trends Comput. Commun.*,no. June, pp. 1111–1117, 2017.

[21] Yan P. and Yan Z., "A survey on dynamic mobile malware detection," Softw. Qual J, no. May 2017, pp. 891–919, 2018, https://doi.org/10.1007/s11219-017-9368-4

[22] Liu X., Lin Y., Li H., and Zhang J., "A novel method for malware detection on ML-based visualization technique," Comput. Secure., vol. 89, 2020, https://doi.org/10.1016/j.cose.2019.101682

[23] Ashawa, Moses & Morris, Sarah. (2019). Analysis of Android Malware Detection Techniques: A Systematic Review. *International Journal of Cyber-Security and Digital Forensics*. 8. 177-187. 10.17781/P002605

[24] Liu, Kaijun&Xu, Shengwei&Xu, Guoai& Zhang, Miao & Sun, Dawei& Liu, Haifeng. (2020). A Review of Android Malware Detection Approaches Based on Machine Learning. *IEEE Access*. PP. 1-1. 10.1109/ACCESS.2020.3006143.

[25] Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., … 0013, F. W. (2021). Malware Detection and Prevention using Artificial Intelligence Techniques. *2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, December 15-18, 2021*, 5369–5377. doi:10.1109/BigData52589.2021.9671434

[26] S. Poudyal, D. Dasgupta, Z. Akhtar, and K. D. Gupta,"Malware Analytics: Review of data mining, machine learning, and big data perspectives," 12 2019.

[27] Budiarto, Raden&Kabetta, Herman &Buana, I Komang. (2020). Hybrid-Based Malware Analysis for Effective and Efficiency Android Malware Detection. 8-12. 10.1109/ICIMCIS51567.2020.9354315

[28] Fedler, A., &Schütte, J. (2019). On the Effectiveness of Malware Protection on Android - An Analysis of Antivirus Apps. In Proceedings of the *4th International Conference on Information Systems Security and Privacy (ICISSP)*.

[29] Zhou, Y., & Jiang, X. (2012). Dissecting Android malware: Characterization and evolution. In 2012 *IEEE Symposium on Security and* Privacy (pp. 95-109). IEEE.

[30] Vidas, T., & Christin, N. (2014). Why phishing works. In Proceedings of the 23rd *International Conference on World Wide Web* (pp. 591-601). ACM.

[31] Baggili, I., &Marrington, A. (2012). Mobile malware. *IEEE Security & Privacy*, 10(3), 80-83.

[32] Microsoft. (2021). Microsoft Security Intelligence Report. Retrieved from https://www.microsoft.com/securityinsights
[33] Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., &Rieck, K. (2014). DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. In *Proceedings of the Network and Distributed System Security Symposium* (NDSS).
[34] Google Play Store. (2023). Retrieved from https://play.google.com/store
[35] Kharraz, A., Robertson, W., Balzarotti, D., &Kirda, E. (2016). Cutting the Gordian knot: A look under the hood of ransomware attacks. In *Proceedings of the 2016 IEEE Symposium on Security and Privacy* (SP) (pp. 574-591). IEEE.
[36] Zhang, Y., Qian, Z., Wang, K., Zhou, X., & Jiang, X. (2013). Vetting undesirable behaviors in Android apps with permission use analysis. In Proceedings of the *2013 ACM SIGSAC conference on Computer &Communications Security* (pp. 611-622). ACM.
[37] Li, P., Wu, Z., Hu, X., Zhang, H., & Li, H. (2017). An empirical study on the effectiveness of malware protection on Android devices. Computers & Security, 70, 99-118

Biographies

Prince Kumar is a research scholar in the Faculty of Computing and Information Technology, Usha Martin University (UMU), Ranchi. He obtained his Master's degree in Cyber Forensics and Information Security from the University of Madras. His research interests include self-destructing messages, Android forensics, and secure backend integration using Firebase and encryption protocols. Prince also holds a certification in Linux and actively researches open-source tools for data extraction and security testing. He has presented international conference papers and is engaged in research pertaining to secure mobile applications.

Dr. Ritushree NarayanPresently serving as an Assistant Professor in the Faculty of Computing and Information Technology at Usha Martin University, Ranchi, Dr. Ritushree Narayan brings with her over 20 years of professional experience. In Computer Science, she also earned her doctorate from Bundelkhand University. Her research interests revolve around Computational Biology, Bioinformatics, and Wireless Sensor Networks. A research-oriented person with a teaching profession, she is an active mentor to students and contributes to the academic development of IT and engineering education.

Dr. Ekbal **Rashid** is currently holding the position of Professor in the Department of Computer Science and Engineering at St. Peter's Engineering College in Hyderabad. He brings more than 20 years of academic and research experience to the table. Another honor in his replete career includes completing a Post-Doctoral Fellowship in Computational and Applied Mathematics from the Technical University of Sofia, Bulgaria, under the almighty supervision of Prof. Nikos E. Mastorakis. He is a Ph.D. holder in Computer Science and Engineering from Siksha 'O' Anusandhan, Bhubaneswar, and also an M.Tech in Computer Science from BIT Mesra. His research interests are Software Engineering, Artificial Intelligence, Machine Learning, and Data Mining..