A Comprehensive Review of Malware Detection, App Permissions and Vulnerability Assessment in Android Security

1st Esha Fatima
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
eshafatima394@gmail.com

2nd Areesha
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
ejazareesha4@gmail.com

3rd Tehreem Amna
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
tehreemamna005@gmail.com

4th Asjad Amin
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
asjad.amin@iub.edu.pk

5th Umar Fayyaz
Faculty of Engineering and Technology
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
umar.fayyaz@iub.edu.pk

***Abstract*—Android devices gaining more and more popularity and have become the all-time-used devices because of their portability nature and are relatively cheap with respect to the other screen devices. This rise in the use of Android devices comes with security challenges as it has grabbed the attention of illegitimate parties who often participate in stealing and compromising the system by using malicious programs. The gaps in this research area must be analyzed to provide valuable insights into the current technological environment.This work illustrates the research landscape by mapping the existing literature to a comprehensive taxonomy, focusing on App Vulnerability Assessments and Machine Learning-based malware detection. This paper provides an analysis of app permissions, scan app vulnerabilities, machine learning-based malware detection, and focuses on user education about security concerns and how they can protect themselves from malicious entities. The improper handling of app permissions contributes to privacy risks and increases in the attack surface. Furthermore,it discusses the credibility of user-installed applications and the need of their access limit to user data. Protects users from malware shared through different files or links using various platforms. Along with the other security techniques, the main idea discussed in this paper is to educate the user on the very common attacks, such as social engineering attacks, and unmanaged app permissions that can be avoided by having prior knowledge of these attacks and that is how users can protect themselves.This review underscores the importance of integrating advanced technologies and user education to build a more secure Android environment.**

***Index Terms*—Malware Detection,App Permissions,Android Security Advisor,Cyber Security**

I. Introduction

Android is a leading mobile operating system worldwide in the first quarter of 2025 and maintained its position with a market share of about 71.88 percent [1], [2].Android's growth is increasing day by day due to its open source nature and the huge amount of freely available applications [3].Due to new technological trends, the use of mobile devices has become a necessity for almost all tasks. A growing number of people depend on their mobile phones for their daily activities, both for personal and professional use. Most mobile applications are developed without maintaining proper security mechanisms and increasing vulnerabilities in the development stage [4]–[6]. Google Play validates the safety status of the application, detects code vulnerabilities and any other malicious behavior of the application before its launch, and mentions the findings in the description to inform the user before installing a vulnerable application, but users do not pay attention to read the description and install them without knowing that their data are at risk [7], [8]. Application Permissions play an important role in limiting the acquisition of user data while app is in use. Users allow both necessary and unnecessary permissions to an application at installation time, and they do not know how to manage the permissions to protect their data. Since permissions are the first thing that any malware will try to exploit,any unnecessary permission of an app works as a backdoor for an attacker to gain access to the mobile [9]. According to a recent McAfee report [1], 2020 was the year of mobile sneak attacks. That is, cybercriminals and state-sponsored actors are persistently seeking ingenious ways to acquire user data. Likewise, every version of mobile comes with new features, which means that it comes with more attack surfaces for attackers, and malware writers that continue to come up with new ways of hiding their attacks and frauds, making it increasingly difficult to identify and neutralize them.

The Android Operating System was released in 2008, and the first malware was detected in 2010, which uses SMS services to target the user by subscribing to a premium service. After that, malware attacks have been on rise, and security attempts have been made to keep user safe from constantly

DOI: https://doi.org/10.67535/tsp.000001.036
Published under the ICACNC 2025 Proceedings

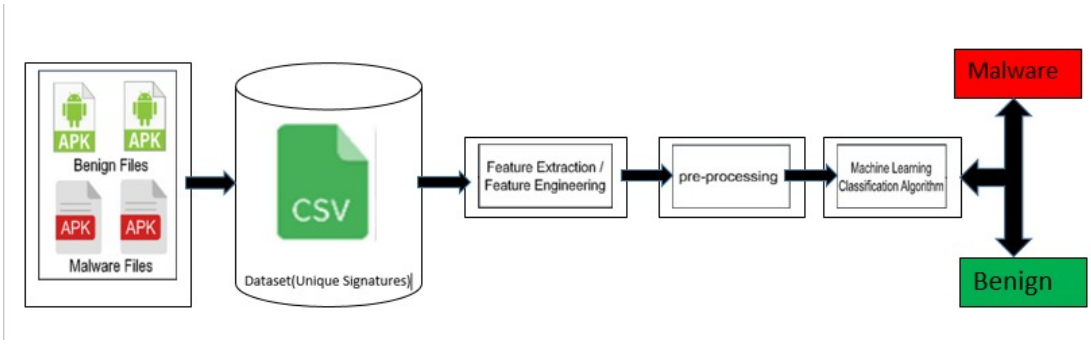

Fig. 1. Machine Learning-Based Malware Detection and Identification System .

increasing of malware attacks. In 2012, the total amount of Android malware is 22,088 and then increases to 33,237,653 until January 2023 [10]. The report in this article [11] shows that the newly found problems come from messaging-based malware, mobile botnets, spyware, trojans, and files or links that are shared through different platforms like "Whatsapp" also contain malicious programs and often generates an alert [12].Mostly, Mobile Applications are used for fulfilling daily life tasks, such as shopping, banking, and social networks. To utilize the features of mobile apps,users also have to share their sensitive information. We investigate how the vulnerability propensity and access level of apps are different from each category of apps. Finally, the solution is to increase the awareness of users about the vulnerability of applications and about data protection [13].

The Google Play store has over 16000,000 third-party Android apps. It has been observed that their individual permission usage has changed over time. Android 6 has changed the way of granting permissions to users, shifting to runtime permission requests instead of install-time permission requests. This is a much needed change; this is based on recent research that users trust the third-party app developers and adversaries and accept all the runtime permissions blindly. Aside from the scope of intentional privacy violations, high-privilege applications increase the attack surface of the smartphone and are more attractive targets for attackers or malware. The focus is exclusively on dangerous permissions, such as those permissions that grant access to sensitive user data by Android. Even at installation time, Google Play also shows the vulnerability point of applications, but users are unfamiliar with the security techniques such as no encryption algorithm is used, access of photo gallery to an banking app and location access. The only thing is to educate users and keep them informed about new threads [14].

II. ML Based Malware Detection in Android

Malware are malicious programs created by the authors of the malware and injected into the system for malicious purposes. When malware starts its executions, harmful activities initialized in the system without the intention and knowledge of the user, such as stealing user credentials, running other programs in the background, and modifying the device setting, are some of the motives that can be achieved. According to(Statista, 2021), the total number of new Android malware samples until March 2020 amounted to 482,579 per month [15] raises concerns about security.

Machine learning algorithms contribute in large scale to detect the anonymity of the program and classify them as malware and benign programs. ML algorithms work by learning the features and patterns that further classify and make decisions about harmful actions. Fig. 1 elaborates the working of the ML algorithm, and describing the work flow, the algorithm compares the file or program with the known signatures of malware stored in the database, processes them, and decides whether the file contains any harmful action and is safe for the user to run. [16], [17].

A. ML Algorithm

Different algorithms involves in different types of detection process. In this paper, we briefly discuss two types of ML algorithm that commonly but effectively used, one is linear regression and the other one is classification, also known as logistic regression. These two algorithms are based on supervised learning which works on labeled data to train the model [18]. Linear regression analysis used to predict the continue variable and explore the relationship between the independent variable and the dependent variable [19], [20] is widely used in business to evaluate trends and make forecast estimates. While, on the other hand, the classification algorithm is used to classify the categories of the object, this algorithm works by creating different groups, learning the different features, and defining or assigning the accurate group to the object based on the features of different categories learned by the model; this model provides a clear concept by making a decision in yes or no, [21], [22]. There are many applications of this algorithm, the classification algorithm plays a very important part in the detection of cancerous cells and malware detection in applications, etc. [23]. To train the model, we split the dataset into two parts. One is for training purpose, this will use 80 percent of the dataset to train the model, training model on large dataset increase the accuracy of the model, the second one is for testing purpose and this will use 20 percent of dataset. Algorithms will be train on training dataset and validate the prediction value by using the testing dataset. Rate

of error will also be extracted by matching the predicted values and the actual value to find the accuracy of the algorithm [15].

This paper presents a review of smartphone security, by focusing on app vulnerability assessments and machine learning-based malware detection. It highlights the importance of proper app permission handling and its impact on user privacy and system security. The study also emphasizes educating users about potential threats and guiding them to identify secure apps and malicious activities.

III. Vulnerability Assessment in Android Apps

In 2019 G DATA Cyber Defence AG(Burris,2020) has reported that over 4.18 million applications were found on the Android platform with round about 11,500 new Android malware evolving on daily basis. An Android application typically follows a structured organization for its configuring the code and resources. The configuration file,"AndroidManifest.xml" contains the app's components, services, activities, permissions and declarations.App permissions helps the users in two ways to protect there access. 1. Resticted data to protect access, like personal information. 2. Resticted actions to protect access, like recording audio.

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
```

Fig. 2. snapshot of the Android Manifest.xml file

Because of the two reasons mentioned above, it has been mandatory to declare the list of permissions by the developers that they are using and the permissions needed by application to perform there functionality or to invoke the Android API successfully. Android has a file that contains a list of all permissions that are required to run the applications efficiently. Permissions are declared by using the ¡uses-permission¿tag within the manifest file. For example, as shown in Fig 2, which is a snapshot of the Android Manifest.xml file of "The WhatsApp Messenger" app, requires permissions such as `READ_PHONE_STATE`, `READ_PHONE_NUMBERS`, `RECEIVE_SMS`, `VIBRATE`, and `AUTHENTICATE_ACCOUNTS` to execute on Android phones. Permissions play an integral role in creating a secure and respecting environment for users privacy . They empower users to control or limit the access to there data , support developers in building secure and trustworthy applications, and contribute to the overall security of the Android platform [24]. Android applications can be downloaded from Google Play and third-party sites.People believe that the applications downloaded from Google Play will be secure, but on some apps Google also shows the vulnerable points in the description of the application, such as no encryption algorithm is used, accessing photos,videos, and the contact list,etc this is a stronge point that Google also provide vulnerable apps to be downloaded [25].

Decompilation:

Use tools like APK Tool or JADX to decompile the APK file, which converts the compiled code into a readable format.

Source Code Review:

Analyze the decompiled code for common vulnerabilities like:

- **Hardcoded Credentials:** Check for usernames and passwords directly embedded in the code.
- **Insecure Logging:** Review logging statements for sensitive data exposure.
- **Insecure Data Storage:** Examine how the app handles sensitive data like user credentials.
- **Lack of Input Validation:** Review if the app properly validates user input to prevent injection vulnerabilities.
- **Unprotected Data Transmission:** Check if data transmitted over the network is encrypted and protected [26].

IV. Challenges in Malware Detection and Vulnerability Detection

As technology progresses day by day and contributes to the security of the user against malicious entities, malware is also shifting their modes, using advanced tools and evasion techniques to avoid the detection mechanism. The zero-day attack, a variety of malware, and an increase in the number of new malware [27] pose significant challenges to Android security.

A. Evasion Techniques

Evasion technique are the methods of delivering the payload to a system without being detected. Polymorphism and metamorphism are the two primary categories used by malware authors to avoid detection [28]. Polymorphic malware can change its appearance while maintaining its functionality and metamorphic malware can completely rewrite its code structure, making detection further complicated. Techniques like these have rendered traditional signature-based approaches less effective and increase the need for the development of more robust detection methods [29].

B. Zero-day Attack

Zero day attack initiated when the developer accidentally leaves an unknown vulnerability in the system which is further used by the intruder to exploit the system and use this to inject malware in the system. Zero day refers towards the time, which mean that the developer and security experts have had zero day to learn about the vulnerability and to provide a patch for the system to prevent the attack and to ensure the safety of data. This rises the challenge of detecting malware in time and protecting the system from any kind of harm. Fig. 3 demonstrate the flow and pattern of this attack, describing the unknown vulnerability existed in the application and exploited by the malicious entity but leaves almost no time for developer to deal with the attack and protect data. [30].

TABLE I
REVIEW OF EXISTING TECHNIQUES FOR ANDROID SECURITY

Ref.	Technique	Dataset/Tool	Findings/Results	Limitations
[11]	Machine Learning (e.g., SVM, RF)	Drebin Dataset, labeled Android apps	Achieved up to 95% accuracy in classifying malware; ML models effectively detect new malware variants	Requires large datasets; limited to static analysis; performance-intensive on mobile devices
[4]	Permission-Based Analysis	AndroidManifest.xml; custom datasets	Identified over-permissioned and privacy-invasive apps; effective in flagging potential risks early	No dynamic behavior tracking; users often ignore permission warnings
[14]	Hybrid Static and Dynamic Analysis (e.g., AndroShield)	Decompiled APKs via JADX/APKTool; runtime analysis	Identified hardcoded credentials, insecure logging/storage, missing input validation	Time-consuming; may miss obfuscated or encrypted logic
[10]	Detection of Advanced Malware (evasion tactics)	Behavior patterns and signatures	Detected polymorphic/metamorphic malware; emphasized advanced behavior-based detection	Signature-based methods are ineffective against evolving variants
[19]	Deep Learning / Privacy-aware ML	Large-scale training datasets; mobile sensors	Improved real-time malware detection accuracy; supported large-scale learning	Raises data privacy concerns; needs high computational power
[26]	Federated Learning	Distributed on-device training (FL framework)	Ensures data privacy by training locally without sending user data to a server	Model inconsistency; limited by device resources and network variability

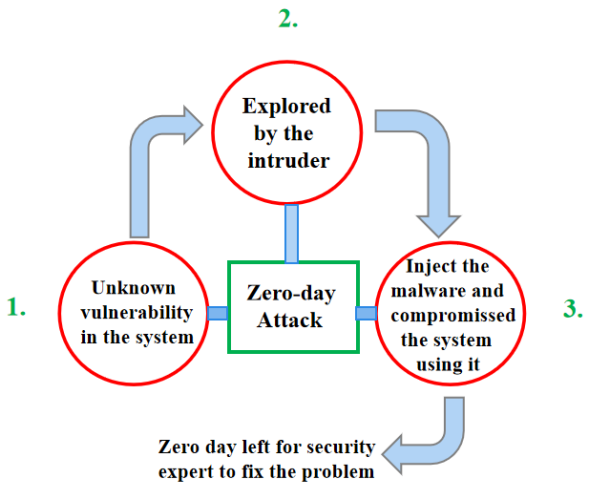

Fig. 3. Zero-Day Attack

C. Variety of malware and increase in rate of new malware

Different type of malware, execute in system differently. Intruders uses variety of malware to harm the system and to breach the user information, some of common malware in android devices are:

- Adware
- Spyware
- Trojans
  - Trojan Dropper, Trojan Banking
  - Trojan Spy
  - Trojan Downloader
  - Trojan SMS
- Backdoor
- Ransomware

Almost 80 percent of the new malware are the variants of the old malware, and the remaining of the 20 percent are unseen malicious programs [27].

Trojan Dropper, also known as roaming mantis belongs to the Wroba group particularly designed for the banking applications, this program breaches the user credentials from the banking applications and harm them financially when it executes in the android devices. Over the year, the execution rate of this malicious program has increased from 2.28 percent to 11.04 percent. This continuous increase in malware's variety and the increased rate of unseen malware have become a challenge in itself in the detection of the malware programs.

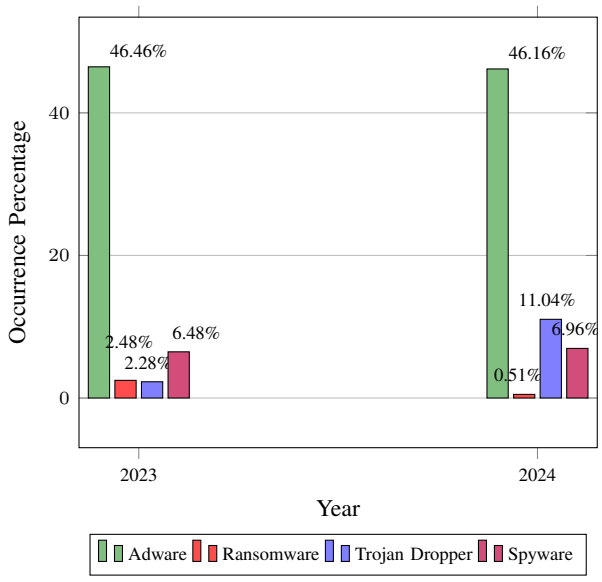

Fig. 4. Comparison of Malware Occurrence in 2023 and 2024

D. Data Privacy Concern

Advanced approaches of machine learning (ML) and deep learning (DL) have been found in the field to address the limitations of traditional malware detection methods. Where

these techniques provide a number of methods to identify malicious behavior within the system, these techniques come with its own challenges. Machine Learning and Deep Learning require a large number of data sets for the model to train for better malware detection and raise the concern about data privacy when collecting and analyzing the large data set of Android applications, potentially compromising user information [31], [32]. The requirement for extensive computational resources and detection time also presents challenges for real-time malware detection on resource-constrained mobile devices [33], [34].

E. Limited Android Resources

Another major challenge in Android malware detection is the trade-off between accuracy and processing expense. More complex machine learning models, such as deep learning approaches, can not only achieve higher accuracy but also require more computational resources and longer processing time. It is important to consider these trade-offs in devices with limited computational resources and battery life, such as mobile devices to maintain a balance between the practical limitations of the mobile environment and the requirement of accurate detection to increase efficiency without compromising performance [34]. This could be achieved by investigating strategies such as feature selection and model optimization [35], [36].

V. Emerging Trends and Future Directions

Emerging trends, and technologies are reshaping the area of cybersecurity, providing advanced tools and techniques to defend against threads.

- Artificial Intelligence and Machine Learning
  - Explainable AI refers to the artificial intelligence and processes or methods that allow human users to understand and trust the results and output created by the machine learning algorithm gaining more popularity in malware detection. Providing transparency in the decision making process, accuracy of malware detection and allowing security professionals to understand the patterns and algorithms used by Explainable AI models. [37]. These kind of AI models help in strengthen the accuracy of virus detection, filtering, immediate response, initialize system alerts against malicious programs in real-time and are designed to work on large number of data set for accurate results.
- Quantum Resistant Encryption
  - Quantum computing uses the unique behavior of quantum physics and mathematics to solve complex problems (fastest computing). The process of decrypting the advance encryption algorithm in seconds has become an easy task with the help of supercomputer and poses a significant challenge in cryptographic methods. Quantum resistant encryption method emerging to avoid attacks performed by quantum computers [38].
- Homomorphic Encryption
  - An advance encryption technique used to secure data during its processing. Homomorphic encryption allow computation on encrypted data without the need of decrypting it first. This technique safely preserve data in storage medium and avoid data temptation [39].
- Federated Learning
  - Performance and accuracy of the model depend on the dataset being used to train the model, however AI models use large number of data to train on and to avoid false negative situation, raises the concern of user privacy when sharing data on multiple devices to train the model. To avoid concerns like data privacy of user an approach known as Federated learning (FL) being used to train models on local devices without sharing the user's personal data with the central server to ensure the privacy and security of the user's information [40].

These techniques are at the forefront and transforming the field of cybersecurity [41]. Moreover educating user and arranging workshops to keep user up to date with evolving threads and attacks has become the need of this time. Having the prior knowledge of the attack help user to mitigate the risk of harming or delving into the attack.

VI. Conclusion

The more in the rise and use of Android device, and the interaction of online services in sensitive areas such as banking sector, storage devices and personal data of user indulge attackers to harm and target this system offensively. This review paper discussed the importance and techniques of malware detection in real time to ensure the safety of system and the information stored in it. Also, common vulnerabilities and some mis-configured settings such as excessive permissions in android device has become one of the reason of attack and data breach are mentioned here. Challenges faced by the traditional malware detection techniques such as variety in malware and the increase in the rate of new malware, evasion techniques, zero day exploit etc has made the detection of malware more complicated.Along with challenges the future considerations and emerging techniques such as the integration of Al and ML models, more advanced and secure encryption techniques such as quantum resistant encryption protect from quantum computing attacks and Homomorphic encryption provide protection during the processing of data, approaches like federated learning to minimize the concerns of data privacy of user arises during the models training on large data set has discussed in this paper to mitigate the challenges. User can protect themself from most common android attacks like phishing and it's variants, Adware, Spyware, Trojans, Ransomware etc by participating or engaging in cybersecurity awareness sessions and workshops.

REFERENCES

[1] A. Sherif. (2025, Mar.) Accessed: 2025-04-01. [Online]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/#:~:text=Android%20maintained%20its%20position%20as,percent%20during%20the%20same%20period.

[2] M. Haris, B. Jadoon, M. Yousaf, and F. H. Khan, "Evolution of android operating system: a review," *Asia Pacific Journal of Contemporary Education and Communication Technology*, vol. 4, no. 1, pp. 178–188, 2018.

[3] W. Zhou, Y. Zhou, X. Jiang, and P. Ning, "Detecting repackaged smartphone applications in third-party android marketplaces," in *Proceedings of the second ACM conference on Data and Application Security and Privacy*, 2012, pp. 317–326.

[4] J. Gao, L. Li, P. Kong, T. F. Bissyandé, and J. Klein, "Understanding the evolution of android app vulnerabilities," *IEEE Transactions on Reliability*, vol. 70, no. 1, pp. 212–230, 2019.

[5] M. E. A. Tebib, M. Graa, P. Andre, and O.-E.-K. Aktouf, "A survey on secure android apps development life-cycle: Vulnerabilities and tools," *International Journal On Advances in Security*, vol. 16, no. 1 & 2, pp. 54–71, 2023.

[6] F. H. Shezan, S. F. Afroze, and A. Iqbal, "Vulnerability detection in recent android apps: An empirical study," in *2017 International Conference on Networking, Systems and Security (NSysS)*. IEEE, 2017, pp. 55–63.

[7] D. Surian, S. Seneviratne, A. Seneviratne, and S. Chawla, "App miscategorization detection: A case study on google play," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 8, pp. 1591–1604, 2017.

[8] N. Viennot, E. Garcia, and J. Nieh, "A measurement study of google play," in *The 2014 ACM international conference on Measurement and modeling of computer systems*, 2014, pp. 221–233.

[9] A. Ehsan, C. Catal, and A. Mishra, "Detecting malware by analyzing app permissions on android platform: A systematic literature review," *Sensors*, vol. 22, no. 20, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/20/7928

[10] Y. Sharma and A. Arora, "A comprehensive review on permissions-based android malware detection," *International Journal of Information Security*, vol. 23, no. 3, pp. 1877–1912, 2024.

[11] J. Drew, "Malware growth maintains rapid pace as mobile threats surge," 2012.

[12] K. Hamandi, A. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, "Messaging attacks on android: vulnerabilities and intrusion detection," *Mobile Information Systems*, vol. 2015, no. 1, p. 746930, 2015.

[13] A. Di Sorbo and S. Panichella, "Exposed! a case study on the vulnerability-proneness of google play apps," *Empirical Softw. Engg.*, vol. 26, no. 4, Jul. 2021. [Online]. Available: https://doi.org/10.1007/s10664-021-09978-0

[14] V. F. Taylor and I. Martinovic, "A longitudinal study of app permission usage across the google play store," *CoRR*, vol. abs/1606.01708, 2016. [Online]. Available: http://arxiv.org/abs/1606.01708

[15] H. Haidros Rahima Manzil and S. Manohar Naik, "Detection approaches for android malware: Taxonomy and review analysis," *Expert Systems with Applications*, vol. 238, p. 122255, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423027574

[16] S. J. Altaha, A. Aljughaiman, and S. Gul, "A survey on android malware detection techniques using supervised machine learning," *IEEE Access*, vol. 12, pp. 173 168–173 191, 2024.

[17] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis, "A signature-based intrusion detection system for the internet of things," *Information and Communication Technology Form*, 2018.

[18] P. Cunningham, M. Cord, and S. J. Delany, "Supervised learning," in *Machine learning techniques for multimedia: case studies on organization and retrieval*. Springer, 2008, pp. 21–49.

[19] L. Jäntschi, L. L. Pruteanu, A. C. Cozma, and S. D. Bolboacă, "Inside of the linear relation between dependent and independent variables," *Computational and mathematical methods in medicine*, vol. 2015, no. 1, p. 360752, 2015.

[20] Y. Shi, "Application of improved linear regression algorithm in business behavior analysis," *Procedia Computer Science*, vol. 228, pp. 1101–1109, 2023.

[21] S. Nusinovici, Y. C. Tham, M. Y. C. Yan, D. S. W. Ting, J. Li, C. Sabanayagam, T. Y. Wong, and C.-Y. Cheng, "Logistic regression was as good as machine learning for predicting major chronic diseases," *Journal of clinical epidemiology*, vol. 122, pp. 56–69, 2020.

[22] X. Song, X. Liu, F. Liu, and C. Wang, "Comparison of machine learning and logistic regression models in predicting acute kidney injury: A systematic review and meta-analysis," *International journal of medical informatics*, vol. 151, p. 104484, 2021.

[23] Z. Akram, M. Majid, and S. Habib, "A systematic literature review: usage of logistic regression for malware detection," in *2021 International Conference on Innovative Computing (ICIC)*. IEEE, 2021, pp. 1–8.

[24] P. Harikrishnan and P. Periyasamy, "A review on the analysis of the effectiveness of permission based security models in android apps," in *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*, vol. 1. IEEE, 2024, pp. 1451–1459.

[25] A. Di Sorbo and S. Panichella, "Exposed! a case study on the vulnerability-proneness of google play apps," *Empirical Software Engineering*, vol. 26, no. 4, p. 78, 2021.

[26] A. Amin, A. Eldessouki, M. T. Magdy, N. Abdeen, H. Hindy, and I. Hegazy, "Androshield: Automated android applications vulnerability detection, a hybrid static and dynamic analysis approach," *Information*, vol. 10, no. 10, p. 326, 2019.

[27] F. A. Aboaoja, A. Zainal, F. A. Ghaleb, B. A. S. Al-Rimy, T. A. E. Eisa, and A. A. H. Elnour, "Malware detection issues, challenges, and future directions: A survey," *Applied Sciences*, vol. 12, no. 17, p. 8482, 2022.

[28] N. K. Gyamfi, N. Goranin, D. Ceponis, and H. A. Čenys, "Automated system-level malware detection using machine learning: A comprehensive review," *Applied Sciences*, vol. 13, no. 21, p. 11908, 2023.

[29] S. K. Smmarwar, G. P. Gupta, and S. Kumar, "Android malware detection and identification frameworks by leveraging the machine and deep learning techniques: A comprehensive review," *Telematics and Informatics Reports*, p. 100130, 2024.

[30] L. Y. Por, Z. Dai, S. J. Leem, Y. Chen, J. Yang, F. Binbeshr, K. Y. Phan, and C. S. Ku, "A systematic literature review on the methods and challenges in detecting zero-day attacks: Insights from the recent crowdstrike incident," *IEEE Access*, 2024.

[31] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Lin, "When machine learning meets privacy: A survey and outlook," *ACM Computing Surveys (CSUR)*, vol. 54, no. 2, pp. 1–36, 2021.

[32] E. Bertino, "Data security and privacy: Concepts, approaches, and research directions," in *2016 IEEE 40th Annual computer Software and Applications conference (cOMPSAc)*, vol. 1. IEEE, 2016, pp. 400–407.

[33] A. McIntosh, S. Hassan, and A. Hindle, "What can android mobile app developers do about the energy consumption of machine learning?" *Empirical Software Engineering*, vol. 24, pp. 562–601, 2019.

[34] T. Zhao, Y. Xie, Y. Wang, J. Cheng, X. Guo, B. Hu, and Y. Chen, "A survey of deep learning on mobile devices: Applications, optimizations, challenges, and research opportunities," *Proceedings of the IEEE*, vol. 110, no. 3, pp. 334–354, 2022.

[35] L. Meijin, F. Zhiyang, W. Junfeng, C. Luyu, Z. Qi, Y. Tao, W. Yinwei, and G. Jiaxuan, "A systematic overview of android malware detection," *Applied Artificial Intelligence*, vol. 36, no. 1, p. 2007327, 2022.

[36] S. Roy, J. DeLoach, Y. Li, N. Herndon, D. Caragea, X. Ou, V. P. Ranganath, H. Li, and N. Guevara, "Experimental study with real-world data for android app security analysis using machine learning," in *Proceedings of the 31st Annual Computer Security Applications Conference*, 2015, pp. 81–90.

[37] A. Saranya and R. Subhashini, "A systematic review of explainable artificial intelligence models and applications: Recent developments and future trends," *Decision analytics journal*, vol. 7, p. 100230, 2023.

[38] R. A. Perlner and D. A. Cooper, "Quantum resistant public key cryptography: a survey," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, 2009, pp. 85–93.

[39] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[40] H. N. C. Neto, J. Hribar, I. Dusparic, D. M. F. Mattos, and N. C. Fernandes, "A survey on securing federated learning: Analysis of applications, attacks, challenges, and trends," *IEEE Access*, vol. 11, pp. 41 928–41 953, 2023.

[41] A. A. Ghaib, "Future trends in cybersecurity: Exploring emerging technologies and strategies," *International Research Journal of Modernization in En-gineering Technology and Science*, 2024.