International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

Exploring Android Security Landscape: Threats, Vulnerabilities, and Best Practices

Akash Rawat[1], Anish Kumar[2], Aman Kumar Singh[3], Dr Kavita Arora[4]
[1,2,3,4]School of Computer Application, MRIIRS, Faridabad, Haryana, India
Emails: *akash890rawat@gmail.com[1], official.anish@outlook.com[2], singhamankumar597@gmail.com[3], kavita.sca@mriu.edu.in[4]*

Abstract
With over 2.5 billion active devices, the Android operating system is among the most popular mobile operating systems. This article looks at the security concerns and challenges it faces. While Android has many advantages, such as numerous customization options and a large app ecosystem, its widespread use exposes it to security flaws and attacks. The article discusses various security threats to Android smartphones, such as stalker ware, SMS phishing, web-based attacks, and fake apps. To improve Android device security, users should exercise caution when downloading apps, enable full disc encryption, careful examine the messages and links, practice safe web browsing, and stay informed about emerging threats. The Stage fright vulnerability, the Humming Bad malware, the Joker malware, and the most recent Flu Bot malware are among the high-profile security flaws that have affected the Android operating system and are discussed in the article. It also lists CVE-2021- 0397 and CVE-2021-0390, two vulnerabilities discovered in 2021, as well as the security updates that were released to address them.
Keyword: *Android, Anti- malware software, Malwares, Security, Security breaches, Threats.*

1. Introduction

Android is a mobile operating system designed primarily for tablets and smartphones. It was founded by Android Inc., which Google later acquired in 2005. With over 2.5 billion active devices since its inception in 2008, Android has outperformed all other mobile operating systems in popularity. One of Android's primary advantages is that it is open-source, allowing developers to modify the operating system's source code and create customized versions. As a result, the Android hardware and software ecosystem has grown significantly and diversely. As a result of its widespread use, Android is a target for security vulnerabilities and online attacks. Malware, phishing scams, and operating system issues are among the most common threats to Android smartphones. As a result, both individual users and enterprises place a high value on Android device security. The popularity of mobile devices is growing due to their portability, ease of use, and growing number of their functions as technology evolves. With this growth, the operating system has undergone significant development and change, laying the groundwork for future addressing Consumer demands. Android, developed by Google, controls the global operating system industry with a massive 70.66% market share, thanks to its popularity on mobile devices. Apple's iOS has a sizable 29.23% market share thanks to its integration with the Apple ecosystem, which is primarily found on iPhones and iPads. The remaining 0.11% is split between several niche operating systems that serve specific industries and purposes, demonstrating the market's diversity (see figure. 1). This research study looks into the various security vulnerabilities that the Android operating system faces. These issues include malware infiltration, phishing schemes, and fundamental flaws in the operating system design. The study investigates the complexities of these security flaws in order to shed light on their implications for Android users. Digital devices are made up of four main components: the user, apps, the operating system, and hardware.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

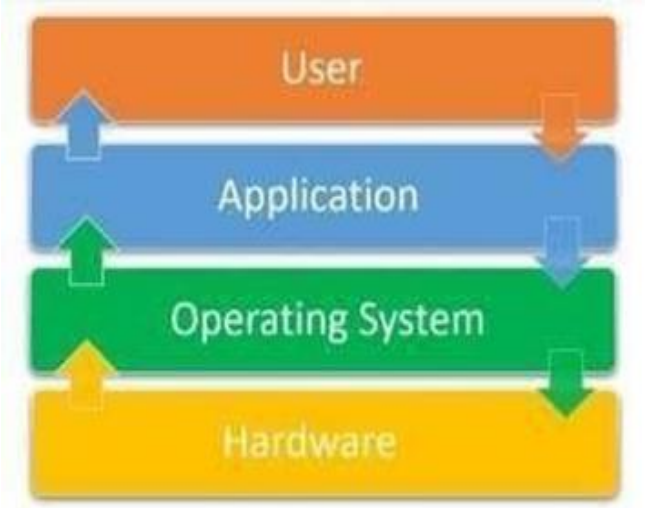

Figure 1 World Wide Market Share of Android

Users are individuals who interact with devices and use software to complete specific tasks. Applications, also known as apps, are software programs designed for a variety of purposes, ranging from work to entertainment. The operating system serves as a go-between, managing hardware resources and allowing applications to run. Hardware refers to the device's physical components, such as the CPU, RAM, and input/output devices, which serve as the foundation for user interaction and app operation. These elements work together to make digital technology function, boosting productivity, communication, and entertainment (See Figure. 2).

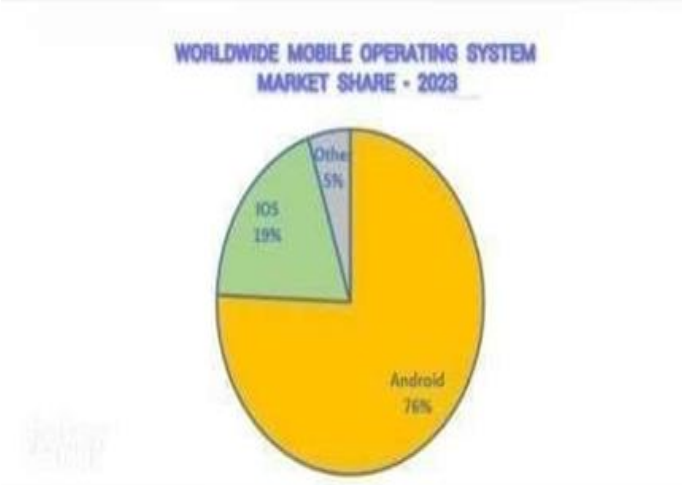

Figure 2 Android Operating System Hierarchical Structure

2. Literature Review

Overlay attacks on Android devices are still a persistent security issue. Animesh Kar et al. [1] propose a detection strategy that combines static analysis and activity behavior examination. Previous approaches attempted to limit overlays at the OS level, but early detection prior to app deployment is critical. Their research contributes by identifying toast overlays in Android apps through component analysis, offering a proactive approach. The evaluation of 4,504 apps shows compatibility with various Android OS versions. The study identifies distinct toast overlays and applies the analysis to Window Manager. Window overlays are based on layout parameters. This study advances understanding and provides a comprehensive detection methodology, emphasizing the importance of taking proactive measures to combat evolving security threats on Android devices.

In their research article [2], Farnood Faghihi et al. address the issue of Android malware in IoT devices. The main issues are a lack of interpretability in malware detection results, increased code complexity, and evasion strategies like obfuscation. The study introduces the Android Interpretable Malware detection technique (AIM) to address these issues. AIM employs neural networks, hybrid analysis, and class modeling to produce clear results and improve malware detection accuracy. This strategy is critical for protecting IoT devices like phones.

Diptiben H. Gillani's [3] study article "A Perspective Review on Malware Detection and Protection" discusses Android's rapid rise in popularity, with a focus on the growing threat of Android malware. Because of Android's open market concept and lack of sufficient security certification, it has been a favorite target for malware developers. The study divides malware detection techniques into static and dynamic categories, with static methods such as signature-based detection and permission-based analysis

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

receiving major attention. It also includes Trojans, Backdoors, Worms, Spyware, Botnets, and Ransom ware as varieties of Android malware. The report, however, contains serious weaknesses, such as a lack of recent market trends, a focus on static analysis, and a lack of viable solutions for developing malware threats.

Shahriar Hassan et al. [4] discuss security threats to Bluetooth technology. This study classifies Bluetooth attacks into three categories based on their severity: high, medium, and low impact. It also delves into Bluetooth malware, distinguishing between Trojans and worms, categorizing them based on their severity and impact on devices. Furthermore, it describes preventative measures implemented by Bluetooth device manufacturers, such as Secure Simple Pairing (SSP) in v2.1 and Secure Connections Only mode in v4.2. The conclusion emphasizes the importance of user awareness in preventing undetected or unreported attacks, highlighting the need for users to learn about Bluetooth threats in order to improve their safety. The information provided highlights the changing nature of threats, the significance of manufacturers' efforts, and the critical role of user awareness in mitigating Bluetooth.

Negi C et al. [5] conducted a review and case study on Android malware, including the threat model, attacks, techniques, and tools. The study discusses Android devices' growing prominence in the smartphone market, as well as growing concerns about their security as malicious apps become more prevalent. It reviews Android components to propose a threat model that depicts potential threats within the Android ecosystem. Furthermore, the paper introduces an attack taxonomy that classifies potential attacks at different layers of the Android architecture. The authors also experiment with feature extraction and classification using machine learning algorithms to detect Android malware.

The research paper "Smart Phone Application Evaluation with Usability Testing Approach" by Naseer Ahmad et al. in [6] discusses usability testing of smartphone applications, with a focus on Android. It introduced the concept of usability testing for smartphone apps, emphasizing the significance of testing the user interface and experience. It emphasizes the difficulties of testing in real-world mobile environments, such as changing environmental conditions and unstable wireless connections. It mentions that traditional usability testing for mobile applications frequently involved laboratory-based testing. It discusses the differences between laboratory and field testing and references some previous studies that compared the two methods. This section delves into the unique challenges of usability testing for smartphone applications issues such as the smartphone's context, connectivity, and screen size, display resolutions and processing capabilities. It discusses goal setting, data collection via interviews, and empirical research, such as user feedback and observations. In a nutshell, the research work sheds light on the challenges and benefits of usability testing while also emphasizing the importance of usability testing in improving smartphone applications.

The research work carried out by Hui-juan et al. in [7] introduced a pioneering framework “MSerNetDroid” for Android malware detection. The authors successfully address the growing threat of malicious attacks on the Android platform by leveraging static analysis and a Multi-Head Squeeze- and-Excitation Residual block (MSer). The proposed model detects malware with an impressive accuracy of 96.48%, outperforming state-of-the-art methods. The emphasis on static analysis and the integration of permissions, API calls, and hardware features in the paper demonstrates its relevance in the dynamic landscape of mobile security. Overall, MSerNetDroid contributes significantly to the field of Android malware detection.

Ahmet Cevahir Cinar et al in [8] meticulously explore the dynamic landscape of mobile security

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

in their comprehensive review paper. The authors deftly dissect the rise in smartphone usage, emphasizing the vulnerability introduced by third-party apps and the growing threat of malware attacks. The paper sheds light on the multifaceted challenges faced by both Android and iOS platforms by thoroughly examining prevalent mobile malwares such as Humming Bad and Pegasus spyware. The authors classify malicious attacks intelligently, from phishing to man-in- the-middle threats, and emphasize the critical importance of addressing mobile vulnerabilities. The review concludes by recommending proactive security measures for users, developers, and network designers, emphasizing the importance of a strong defense against the rapidly evolving mobile threat landscape.

Diptiben Ghelani's research paper examines the changing landscape of Android malware threats and the resulting increase in malware protection mechanisms. Ghelani's two-part contribution includes a thorough examination of Android malware and sophisticated penetration techniques, as well as an evaluation of antivirus software designed to protect Android systems. The paper categorizes recent antimalware techniques according to their detection methods, providing a concise but insightful overview of the ever-changing field of malware detection and protection mechanisms. Ghelani also forecasts Android market trends through 2018, offering valuable insights to stakeholders. A notable contribution is the development of a novel hybrid security solution for Android applications that emphasizes the balanced integration of static and dynamic analysis. [9]

3. Previous High-Profile Android Security Breaches

Security breaches refer to an unauthorized access, disclosure, or compromise of confidential information or systems, potentially resulting in data loss, damage, or misuse. It denotes a breach in security, allowing unauthorized individuals or entities access to sensitive data or resources. Given below are the previous high profile security breaches [10]:

3.1. CVE-2021-0390 (August 2021)

Google has released a security patch for Android devices that addresses a major vulnerability in the operating system's System component. The CVE-2021-0390 vulnerability allows for remote code execution on a victim's device [11].

3.2. CVE-2021-0397 (October 2021)

A flaw in the Android operating system has been discovered, potentially giving hackers access to a user's smartphone. The CVE-2021-0397 vulnerability, which affects Android 10 and 11, could be exploited by malicious software to cause harm [12].

3.3. FluBot (December 2021)

In Europe, Android smartphones were discovered to be infected with a malware strain known as "FluBot." The software, which is distributed through SMS phishing campaigns, is designed to steal sensitive data such as banking passwords and personal information [13].

3.4. CVE-2022-21318 vulnerability (February 2022)

An attacker could exploit this vulnerability in the Android System component to execute arbitrary code on a victim's device. Google issued a security patchto address the issue [14].

3.5. CVE-2022-35251 vulnerability (June 2022)

This flaw in the Android System component may enable attackers to gain local privilege escalation on a victim's device. Google issued a security patch to fix the problem [15].

4. Attacks and Security Threats in Android Operating System

The Android operating system has been a popular target for security threats and assaults because to its widespread adoption on a wide range of devices various risks and potential dangers that can threaten the confidentiality, integrity, and availability of data on Android devices. These threats can take various forms and target system vulnerabilities or user behavior: Comparison chart (See Table 1).

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

4.1. Stalker Ware

Stalker ware is a type of malware that tracks an individual's Android device activity without their knowledge. Monitoring of location data, text messages, and phone logs is commonly used. Stalker ware's potential implications extend beyond invasion of privacy to stalking, harassment, and even data breaches. Users can protect themselves from this insidious threat by regularly evaluating their installed apps, limiting Android's permissions, and using reputable anti-stalker ware software [16].

Table 1 Comparison Chart of Android Security Threat

Threat	Definition	How it Woks	Impact on the system
Stalker ware	Stalker ware is a type of malware that secretly monitors an individual's Android device activities, such as location data, text messages, and phone logs.	Stalker ware infiltrates a user's device, often disguised a s a legitimate app, and collects personal information invisibly.	Stalker ware can result in privacy invasion, stalking, harassment, and potential data breaches. Users can protect themselves
SMS Phishing	SMS phishing, also known as smishing, is a deceptive technique in which attackers send fraudulent text messages to users in order to trick them into disclosing sensitive information or clicking on malicious links.	Text messaging is used by attackers to send deceptive messages, often posing as a trusted entity, prompting users to take actions that compromise their security.	Smishing can lead to the unintentional disclosure of sensitive information. Users should be cautious, double-check sender information, and avoid link .
Web Based Attacks	Web-based attacks on Android devices take advantage offlaws in online browsers, apps, and websites, resulting in data theft and malware infections.	Attackers target flaws in online platforms in order to compromise user data. Exploiting unpatched software or duping users into visiting malicious websites may be involved.	Data breaches and the installation of malicious software can occur as a result of web- based attacks. Users should exercise caution when using the internet, keep their software up to date, and avoid suspicious websites and downloads.
Fake App	Fake apps imitate legitimate apps and are frequently distributed through platforms such as the Google Play Store. These apps may contain malicious code, which could result in malware infectionsand data breaches.	Cybercriminals create fraudulent apps that look like popular and trusted apps in order to entice users to download them. These apps, once installed, may harm user data and device security.	Malware infections and unauthorized access to sensitive information can be caused by fake apps. Users should only download apps from reputable sources, carefully examine app permissions, and think about using mobile security solutions.

4.2. SMS Phishing

SMS phishing, also known as smishing, is a deceptive tactic in which attackers send fake text messages to trick consumers into disclosing sensitive information or clicking on dangerous links. Smishing has grown in popularity among

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

cybercriminals, who continue to use text messaging as a primary means of communication. To reduce this risk, users should be cautious when receiving unsolicited messages, verify sender information, and avoid clicking on unexpected links [17].

4.3. Web-based Attacks

Web-based attacks against Android devices are on the rise. These attacks frequently exploit flaws in online browsers, apps, and websites, resulting in data theft, malware infections, and other criminal activity. Users are encouraged to use the internet with caution, to update their browsers and programs on a regular basis, and to avoid questionable websites and downloads [18].

4.4. Fake Apps

While the Google Play Store is a reliable source for apps, it is not immune to fraudulent and malicious applications. Fake apps pose as legitimate ones, enticing users to download them. These apps may contain malicious code, which can lead to malware infections and data breaches. To combat this threat, users should only download apps from trusted sources, carefully examine app permissions, and consider using mobile security solutions for added protection [19].

5. Enhancing Android device Security

Android device security refers to the policies and procedures in place to safeguard Android- powered smartphones, tablets, and other devices running the Android operating system against unauthorized access, data breaches, and malicious activity. The following are important aspects of Android device security:

5.1. Exercise Caution with App Downloads

Users should follow certain guidelines when downloading apps to reduce the possibility of downloading malicious applications. Only download apps from reputable sources, such as the Google Play Store, as they have been thoroughly vetted. Before installing, review the requested app permissions, as well as the user reviews and ratings.

5.2. Enable Full Disk Encryption

Turn on full disc encryption on your Android device. This feature encrypts data on the device, rendering it unreadable without the appropriate decryption key. This safeguard protects sensitive information from loss or theft.

5.3. Examine Messages and Links

When receiving unsolicited text messages, use caution and avoid clicking on unknown links. Check the sender's authenticity and be wary of phishing attempts

5.4. Be Mindful of Web Browsing

When using an Android device to access the internet, be cautious of potentially harmful websites. Maintain safe browsing habits and avoid downloading files from untrustworthy sources.

5.5. Educate Yourself and Stay Informed

Keep up to date on the latest Android security threats, trends, and best practices. It is critical to keep one's knowledge about emerging threats and defense strategies up to datein order to keep an Android device secure.

5.6. Enhancing User Security

Android's Built- In Safeguards Built-in safeguards are the security features and measures that the Android operating system includes to protect devices and user data. These safeguards are intended to provide a basic level of security while mitigating a wide range of possible threats. Here are some of the most Android's built-in safeguards:

5.6.1. App Sandboxing

App sandboxing is a technique used by Android to isolate apps and prevent them from accessing each other's data or code. According to this, if only one app on the smartphone is compromised, the attacker will be unable to access other apps or data.

5.6.2. Permissions System

Android's permissions system requires apps to request permission before accessing specific data or resources, such as the device's camera or microphone. Users must give an app permission to access these resources. Users may revoke their permission at any time. Permissions in the Android operating system are divided into two categories: normal and dangerous.

5.6.3. Normal Permissions

Normal Permissions, such as accessing the internet, using fingerprint scanners, or enabling NFC for functions such as mobile payments, are provided

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

immediately upon app installation and pose low privacy threats.

5.6.4. Dangerous Permissions

Dangerous permissions, on the other hand, such as access to contacts, location, microphone, or SMS, are deemed high- risk and require specific user approval at runtime (See Figure 3). This distinction allows users to make informed decisions about sensitive data access, while app developers in the Android ecosystem balance functionality and privacy, influencing the dynamic landscape of mobile application security and user data protection.

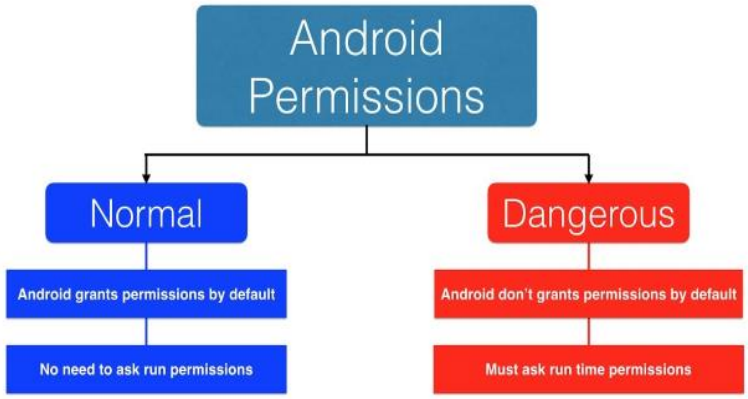

Figure 3 Partitioning Android Permission

5.7. Data Encryption

Android uses data encryption to safeguard user information on the device. This means that even if someone gain access to the device, they will be unable to read or access the data unless they know the encryption key.

5.8. Two-factor Authentication

Android supports two-factor authentication, which increases the security of user accounts. To access their accounts, users must provide a second form of authentication in addition to their password, such as a fingerprint scan or a code sent to their phone.

5.9. Secure Boot Process

Android has a secure boot process that ensures that only trusted software is loaded onto the device during the boot process. This prevents attackers from loading malicious software onto the device during start-up.

6. Result

An extensive investigation revealed critical insights into Android security, shedding light on a variety of vulnerabilities encountered by users in their daily interactions with the platform. These flaws include undetected malware infiltrations, complex phishing schemes, and operating-system design flaws. The study meticulously exposes the complex web of security issues that Android users face. The widespread use of Android, combined with the ever-expanding mobile device landscape, emphasizes the critical importance of device security. This critical need extends beyond individual users to businesses and enterprises that rely heavily on Android-powered devices for a wide range of tasks. In today's digital landscape, device security is clearly prioritized. The rapid adoption of Android, combined with the continued expansion of the mobile device ecosystem, emphasizes the critical need to protect these devices. This is especially important for businesses and organizations that rely heavily on Android-powered devices for a variety of purposes. In today's digital world, ensuring the security of these devices is clearly a top priority. This study suggests practical measures you can take to improve Android device security. These include exercising caution when downloading apps enabling full disc encryption, inspecting messages and links, engaging in safe web browsing, and staying current on emerging threats and best practices. Finally, it is critical to highlight the significance of learning from previous high-profile Android security breaches. These incidents serve as cautionary tales,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

emphasizing the ever-changing nature of the security landscape and the ongoing importance of proactive security measures.

Conclusion

This study highlights the critical need to address security flaws in the Android operating system. As Android continues to take control of the mobile device market, there is an obvious need for robust security measures. Examining built-in safeguards and user best practices provides a comprehensive picture of the security environment. Individuals and businesses can effectively protect their Android devices by understanding the risks and taking the recommended security precautions. Previous security breaches serve as stark reminders of the ubiquity of threats in the digital age. Finally, this research contributes to the security and resilience of Android devices in a constantly changing and dynamic technological environment.

Future Scope

This study shed the spotlight on the existing security flaws in the Android operating system, and there are several promising directions for future research in this area. One area of focus could be on developing advanced malware detection techniques that can keep up with changing attack strategies. Furthermore, it is critical to investigate new approaches to securing Android's open-source nature while maintaining customizability. Future research could go deeper into improving user education and awareness of best security practices. With Android's rapid evolution and a growing threat landscape, ongoing research is critical for effectively adapting and responding to new challenges. Collaboration between academia and industry could result in innovative Android security solutions. By staying proactive and adaptable, we can collectively fortify the security of android devices in an ever- changing digital landscape.

References

[1]. Kar, A., Stakhanova, N., & Branca, E. (2024). Detecting Overlay Attacks in Android. Procedia Computer Science, 231, 137144.https://doi.org/10.1016/j.procs.2023.12.18 5.

[2]. Faghihi, F., Zulkernine, M., & Ding, S. (2023). Aim: An android interpretable malware detector based on application class modeling. Journal of Information Security and Applications, 75, 103486.

[3]. Ghillani, D., & Gillani, D. H. (2022). A perspective study on Malware detection and protection, A review. Authorea Preprints.

[4]. Hassan S S, Bibon D S, Hossain S M, Atiquzzaman M, Security threats in Bluetooth technology Computers & Security.https://doi.org/10.1016/j.cose.2017.03.008

[5]. Negi, C., Mishra, P., Chaudhary, P., & Vardhan, H. (2021). A review and Case Study on android malware: Threat model, attacks, techniques and tools. Journal of Cyber Security and Mobility, 231-260.

[6]. Ahmad N, Boota M and Masoom A (2014) Smart Phone Application Evaluation with Usability Testing Approach. Journal of Software Engineering and Applications, 7, 1045-1054. doi: 10.4236/jsea.2014.712092.

[7]. Zhu H, Gu W, Wang L, Xu Z, Sheng V, Android malware detection based on multi-head squeeze-and-excitation residual network, Expert Systems with Applications, Volume 212,2023,118705,ISSN.

[8]. Cinar, Cevahir A, and Kara T B, "The current state and future of mobile security in the light of the recent mobile security threat reports." Multimedia Tools and Applications (2023): 1- 13.

[9]. Ghelani D, A perspective study on Malware detection and protection, A review authored, September 13, 2022.

[10]. Wang, X. (2022). Security Threats and Protection Based on Android Platform. In 2021 International Conference on Big Data Analytics for Cyber-Physical System in Smart City: Volume 2 (pp. 179-186). Springer Singapore.

[11]. Mourya, D., Srivastava, S., Pal, D., & Dehraj, P. (2022). A Survey: Android

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0271
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 1831-1839

Architecture and Security Threats. In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2022 (pp. 707-719). Singapore: Springer Nature Singapore.

[12]. Khan, S., Yusuf, A., Haider, M., Thirunavukkarasu, K., Nand, P., & Rahmani, M. K. I. (2022, June). A Review of Android and iOS Operating System Security. In 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (pp. 67-72). IEEE.

[13]. Sharma, T., & Rattan, D. (2023). Android malwares with their characteristics and threats. In Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022 (pp. 1-12). Singapore: Springer Nature Singapore.

[14]. Ruchita T, Sanjitha V, Chowdary G S, Chakradhar A D S, Anuraj D K and P. K, "Malware Detection in Mobile Phones," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1096-1102, doi: 10.1109/ICICT57646.2023.10134097.

[15]. Yadav, Shekhar C, and Gupta S. "A Review on Malware Analysis for IoT and Android System." SN Computer Science 4.2 (2022): 118.

[16]. Gürkan Balıkçıoğlu, P., Şırlancı, M., ACAR KÜÇÜK, Ö. Z. G. E., Ulukapi, B., Turkmen, R. K., & Acartürk, C. (2022). Malicious code detection in android: the role of sequence characteristics and disassembling methods.

[17]. Gencer, K., & Başçiftçi, F. (2023). Analysis and Modeling of Android Software Vulnerabilities: A Numerical Approach.

[18]. Diptiban G, and Gillani D H. "A perspective study on Malware detection and protection, A review." Authorea Preprints (2022).

[19]. Sharma T, and Rattan D, "Android Malwares with Their Characteristics and Threats." Mobile Radio Communications and 5G Networks: Proceedings of Third MRCN 2022. Singapore: Springer Nature Singapore, 2023. 1-12.