International Journal of Engineering and Applied Computer Science (IJEACS)
Volume: 03, Issue: 01, December 2021

Smartphone Security and Protection Practices

Mohammed Abdul Bari
Department of Computer Science and Engineering, ISL Engineering College, Osmania University, Hyderabad, India
Email: bari_bari11@rediffmail.com

Shahanawaj Ahamad
College of Computer Science and Engineering, University of Hail, Hail City, Saudi Arabia
Email: drshahwj@gmail.com

Mohammed Rahmat Ali
Department of Computer Science and Engineering, ISL Engineering College, Osmania University, Hyderabad, India
Email: rahmat_ali2u@yahoo.com

***Abstract*—The research and communications for detecting mobile security threats with the best protection practices of applications have become essential goals nowadays due to the continuous discoveries of new vulnerabilities. The internet and web-based activities have been increased drastically in recent times by users of all categories. Users have extensively started involved in gaming, banking, frequent bill payment, entertainment, and other network and online activities that are requiring a large number of mobile phone protection and security mechanisms in response to advancements in full-stack applications and wireless networks. The goal of this paper is to uncover the best-applied practices in the domain of mobile security to protect smartphone devices. The main advantages of smartphones are small size with easiness in carrying anywhere and can be a replacement for computing devices in some ways for example emails. Unfortunately, the convenience of using smartphones to do the private task is the loophole cyber attackers need to gain access to personal data. Thus, this paper proposed eight best practices to protect and secure smart mobile phones.**

Keywords — ***Smartphone, Mobile Security, Mobile Protection, Intelligent System.***

I. INTRODUCTION

The recent age is well thought-out as the age of mobility and network communication. To be in touch for long-distance, no need to be hung around for days or hours; nowadays the mode of communication is almost in real-time. The fast and accelerated innovations in information and communication technologies and mobile devices in current years have made it possible. From the early nineteenth century till date, the development of mobile devices boosts extraordinarily [1, 2].

In 1947[1], Bell laboratory introduced the word Mobile Network and the first automated mobile phone systems scheme for private vehicles that was launched in Sweden in the year 1956. The first money-making commercial mobile phone was introduced by Motorola. In 1973, they made the first public mobile phone call on a device that was weighed 1.1 Kg [1].

In the history of 30 years, there were some foremost changes in the mobile phone architecture. Numerous revolutions had been occurring in that era, which is reported in the figure 1. [1, 2, 3, 18].

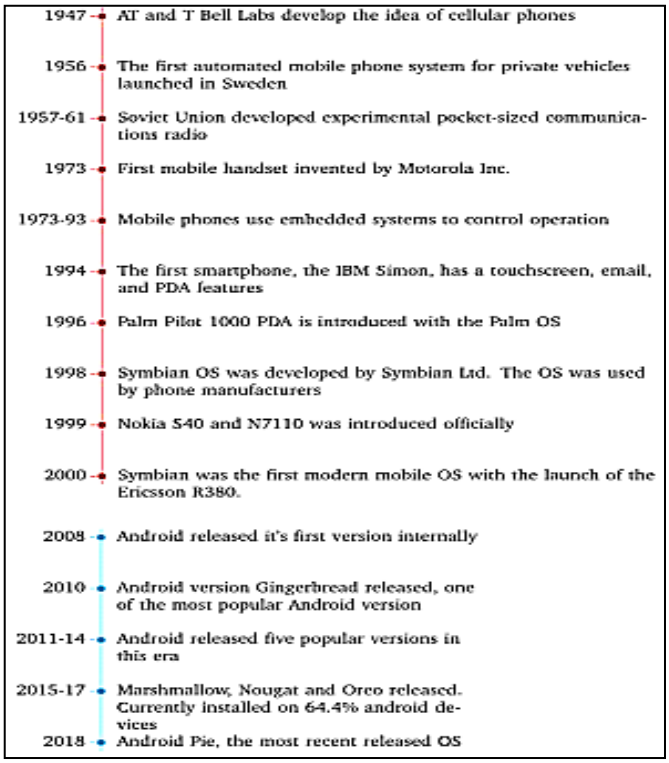

Fig.1. Evolution of Mobile Device & OS [1]

II. BACKGROUND STUDY

The latest researches have shown a significant rise in the popularity and ubiquity of mobile devices among all categories of users all around the world [4]. Devices are based on an explicit operating system either Android or iOS that enables users to install a huge variety of applications, usually referred to as "apps," from online sources called markets: Apple App Store, and Google Play [4, 5]. The aforementioned apps are the core of smartphones that are elevating their functionality and enhancing the daily lives of their users. The app markets permit users to carry out a quick search and put in new apps, but at the same time, they are also a starting place of different kinds of malware masked as normal apps. Nowadays, mobile devices are subject to a wide range of safety challenges and malicious threats. [6,7,20]

Today, every smartphone operates based on its operating system. Android, iOS, Tizen, KaiOS are the main of this type [3]. This smartphone Operating System (OS) allows added software to run on the phone to which provides varied functionalities to the users. It enhances the user knowledge, but security and privacy are the main concern to worry by allowing 3rd party apps on users' devices. As a result, smartphone OS developers don't want to allow 3rd party apps to access root level and susceptible information. Being a flexible smartphone OS at the beginning, Google's Android is also following the warning access method. Accessing system-level information, system logs, and other susceptible information is now being restricted continuously. In our studies, we have found that the development of many machines' optimization and security-related apps had stopped due to permission decline. [1, 2, 3]

There are a few studies that work on Android's security problem in the app development and adjustment phase. Jha et al. [8] studied 13,483 real-world Android applications and found only 2,373 apps with no configuration errors; this is a development phase scenario. These security problems become more severe when studies establish that security and privacy are not the main tasks of the developers [3]. Security and privacy are common responsibilities of both the app service providers and the end-users. Usage-pattern and misuse: both intentionally and unintentionally may raise the probability of security threats to the end-users. Google's Android help and support center provide some simple guidelines for the Android device users for helping the device and information safe and secure [9, 1, 3, 22]

According to researchers and agencies, mobile computing is a phenomenon worth observing since our habits as consumers, a few of which are listed in the following and are radically changing [7, 10, 11, 12]:

- Over 73%, depending on any age group, of all emails are opened on mobile devices.
- Already in 2017, around 95% of Facebook users accessed the social network via mobile devices.
- 80% of users used a mobile device to search the internet in 2019.
- 40% of online transactions are done using mobile devices.
- More than 50% of websites now use responsive web design technologies that work for all devices.
- More than 75% of shoppers use mobile devices along with physical shopping.
- Global mobile data traffic is more than 30 exabytes per month.

The figure for mobile subscriptions shown in Figure 2 rises at 3 percent year on year and currently totals around 8 billion. High subscription growth continues from previous quarters in China, which had the most net additions during the quarter (+14 million), followed by Indonesia (+9 million) and the Philippines (+8 million).

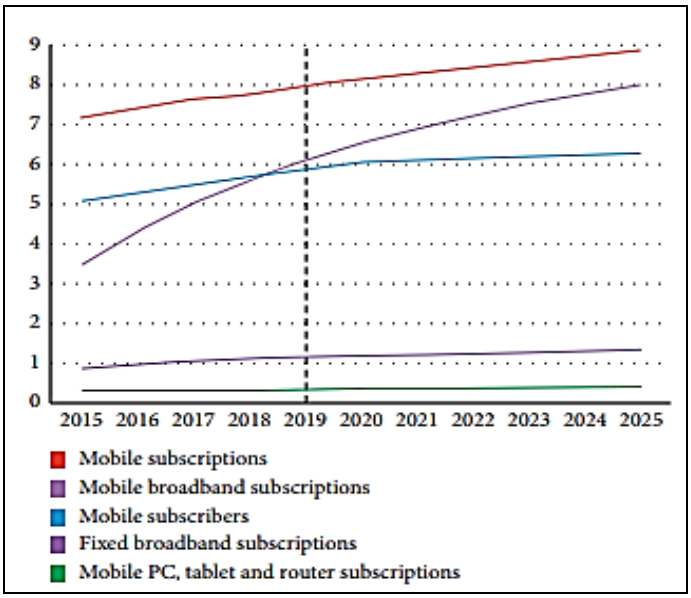

Fig.2. Global mobile subscriptions and subscribers (in billions) [10]

The figure for mobile broadband subscriptions raised 10 percent year-on-year, growing by 120 million in Q3 2019. The total is at the present 6.2 billion or 77 percent of mobile subscriptions. Figure 3 for 4G (LTE) subscriptions amplified by 190 million for the period of the quarter to reach a total of 4.2 billion, or 52 percent of all mobile subscriptions. 3G (WCDMA/HSPA) subscriptions were rejected by 50 million and 2G (GSM/EDGE-only) subscriptions were rejected by 70 million. Other technologies to reject by around 10 million [4,10].

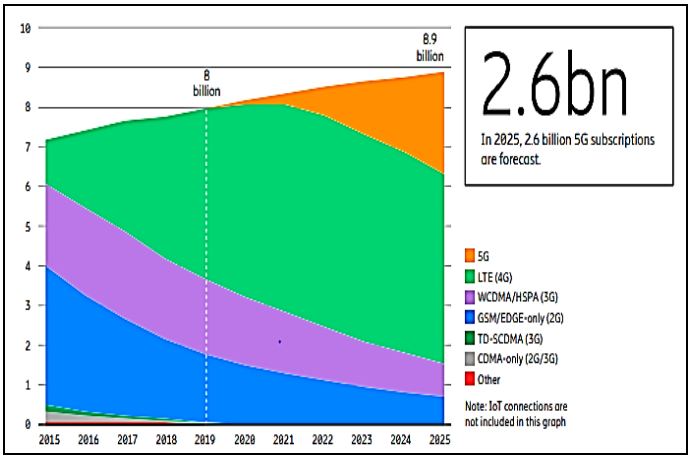

Fig.3. Mobile subscription by Technology (in billions) [4, 10]

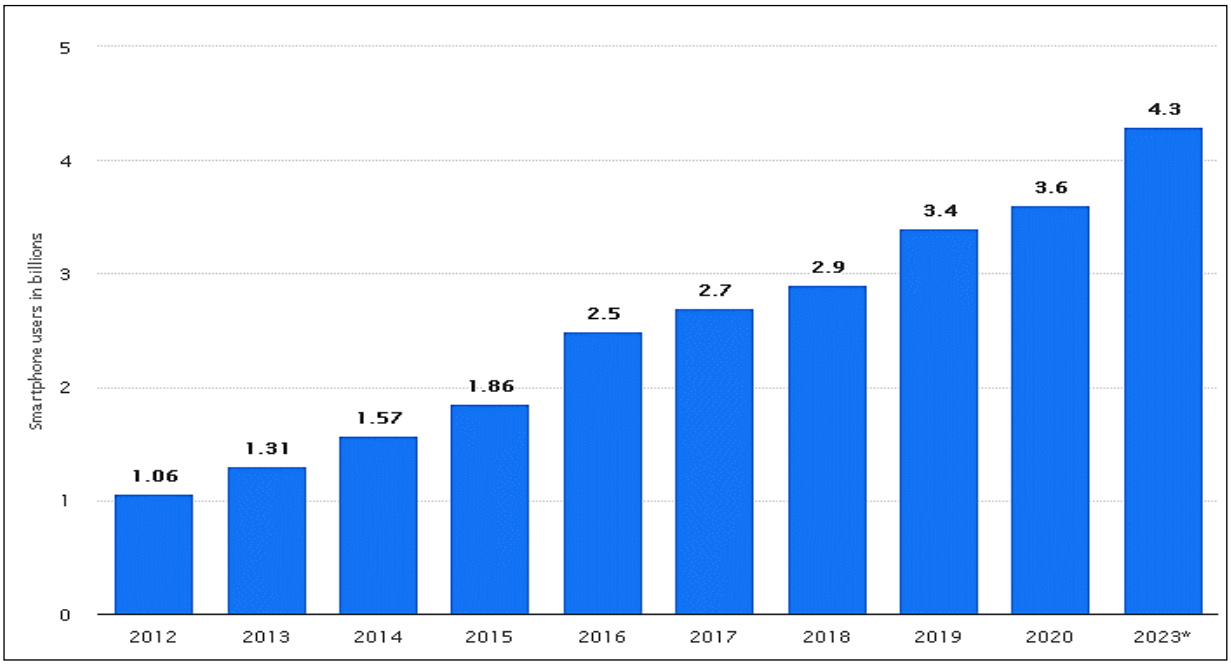

Fig.4. Number of Smartphone users worldwide 2012-2023 [4,10]

Figure 4 depicted the number of smartphone users worldwide, which nowadays surpasses three billion and is forecast to further grow by numerous hundred million in the next few years. China, India, and the United States are the countries with the maximum number of smartphone users, with a collectively 1.46 billion users. The Smartphone market still has high growth possible though, as the Smartphone diffusion rate is still lower than 70 percent in many highly occupied countries, in particular China and India.

Figure 5 has depicted the mobile applications worldwide. The revenue of the global Smartphone market continuous to boost over the last few years, despite stagnating unit sales, due to a growing average promotion price of smartphones. [4,10] The foremost Smartphone vendors today are Samsung, Apple, and Huawei. Taken jointly the three knowledge companies account for about half of all smartphone shipments worldwide. All three shipped at least 200 million smartphones in 2018, with Samsung leading the way with more than 290 million Smartphone unit shipments. [4, 10]

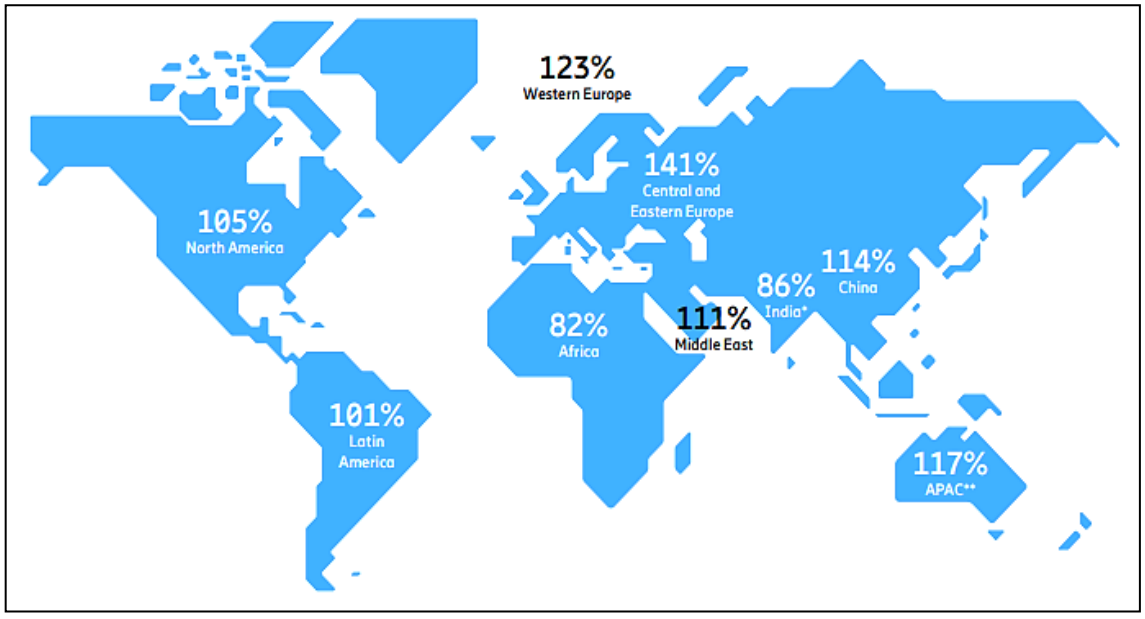

Fig.5. Mobile Application around the globe [10]

III. SMARTPHONE PROTECTION SECURITY PRACTICES

Security is being widely discussed in the field of application development with improving quality for end-to-end consumer satisfaction at different levels. On the contrary, at some stages the security requirements typically force barriers to users (such as passwords or other authentication mechanisms), while designers and developer's effort to minimize their impact on both application performance and user experience [7]. Figure 6 has depicted the best practice model for smartphone security and threat protection.

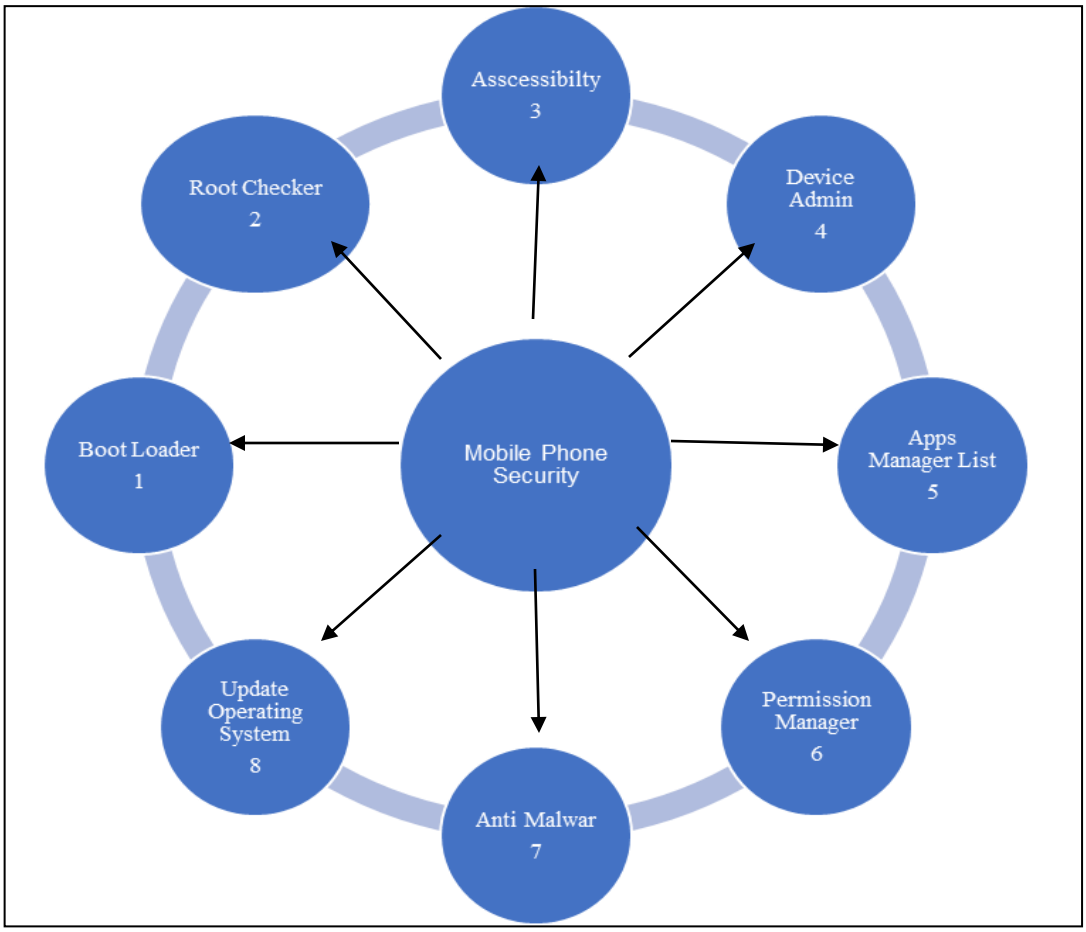

Fig.6. Best practice to protect smart mobile phone.

A. *Boot Loader*

The bootloader is the primary activity that starts up when a phone is turned on. Its most basic level, a bootloader is the low-level software on the smartphone that keeps you from breach it. It is used to make sure and verify the software running on your phone before it loads. Think of it, like a security to your phone. Whether you're allowed to unlock your bootloader it depends on the manufacturer of your phone, the model you have, and even your carrier. If you were to try to load software onto the phone that was not properly signed by the device vendor, the bootloader would detect that and refuse to install it on the device. [13]

If the bootlaoder is open don't used the phone. As its EMI Number might be change or phone might be stolen. In order to check bootlaoder restart the phone and check any sign of warning, in starting stage.

B. *Root Checker*

It is a method of unlocking an Android device in regulates to grant the user privileged control, or root access. It's a lot like having administrator privileges on a Windows or Linux-based OS.

A lot of users want to root Android smartphones so as to they can put in various third-party apps or conquer certain system limitations, usually put in place by hardware manufacturers and carriers.

- *Go to Settings of your phone → tab About Phone → in that Status Information → Check Device Status.*

Official means that the software has not been tampered with and the device is not rooted. If seeing a custom tag beneath device status typically means that your phone is rooted. The Root Checker app is a third-party app that you can download for free from Google [14] and if this application says your phone is rooted, then its trouble, if this application says it's not rooted, then its fine.

C. *Accessibility*

In Accessibility which we can find in sitting of our mobile, every think should be off. We can't give permission to any app, which uses our Audio or Video without our permission.

- *Go to Sitting → Top Search Accessibility → ones it is open, check in that every think should be off.*

D. *Device Admin or Device Manager*

The steps.

- *Select "Security" from the Settings Menu-Scroll down and tap "Device administrators" Ensure that "Android Device Manager" is checked.*

Except find my device, any other app is there, that should be delete it.

E. *Apps Manager List*

As soon as you have an Android phone, we can't wait to install your favorite apps on it. The apps can be regarding games, media player, bookstore, social, business. The Android App Manager is an Android Management tool which helps to administer all apps installed on your Android phone. It can illustrate you the information about an app, rapidly search any app installed, and offer a detail to tell you the frequently used apps and unused apps and more.

Check of unused apps as well trusted apps names which you haven't used for lengthy time, select that apps and click to uninstall them. [15]

F. *Permission Manager*

Android apps will request for permission when you download some apps. In Permission Manager check how numerous Apps using your Camera, Contract, Photos, Locations, Microphone etc. The figure 7 of particular Mobile has shown below, deny permission which you don't want it. Whenever you are using give permission otherwise don't give. If you don't have permission manager in your phone, download it form Play Store.

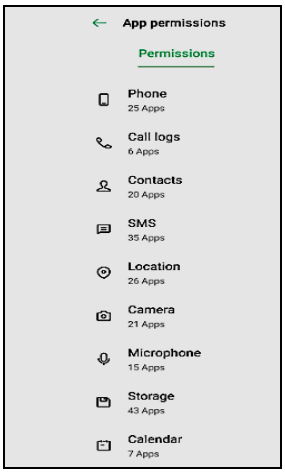

Fig.7 App permissions

G. *Anti-Malware*

Malware attacks have been rising quickly from last 10 years; these attacks targeted all technology device as well as mobile phones. Due to the behavior of the mobile usage and the responsive data they might contain, safeguards against malwares, Anti-Malware or Anti-Virus must be installed in our mobile phone, and it should be updated. [16, 21]

H. *Update Operating System*

Update mobile operating systems and on-board applications with safety patches: keeping the operating system (Android and iOS) and the installed applications up to date is a must. Both Google and Apple provide regular updates to users, which resolve recent vulnerabilities or other threats, as well as sharing additional performance and security features [17].

In addition to above point

- Back up your data regularly.
- Disable Bluetooth and Wi-Fi when not needed.

IV. CONCLUSION

Security is forever is type of an arms race connecting attackers and defenders. Since the mobile application market is rising, at the same time, mobile security will carry on bringing an excess of issues to countenance. In other words, security is often a substance of opposite risk and reward, as discussed during the World Economic Forum of 2019. The participants came to the wrapping up that the past ten years score only the start of the worldwide cybersecurity trip. New architectures and collaboration are still required as we need to stand to face risk at the brink of a new era of cybercrime, which will be empowered by new and developing technology. These four technologies, namely, 5G networks, infrastructure convergence, artificial intelligence, and biometrics, are going to change the next ten years of global cyber and smart devices security.

REFERENCE

[1] Ratul Sikder , Md Shohel Khan , Md Shohrab Hossain , Wazir Zada Khan," A survey on android security: development and deployment hindrance and best practices", TELKOMNIKA Telecommunication, Computing, Electronics and Control, Vol. 18, ISSN: 1693-6930, February 2020.

[2] uSwitch Mobiles, "History of mobile phones," Available: http://bit.ly/2SfFmwu, Accessed: 11 March 2019, April 2018.

[3] ShoutMeLoud, "Top 10 mobile phones operating systems," [Online], Available: http://bit.ly/2Y2KREh, , November 2017

[4] Statista, Smartphones—Statistics & Facts, Statista, Hamburg, Germany, 2020, https://www.statista.com/topics/840/ smartphone

[5] B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, "Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review," IEEE Access, vol. 7, pp. 68557–68571, 2019.

[6] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," IEEE Access, vol. 4, pp. 4543–4572, 2016.

[7] Paweł Weichbroth & Łukasz Łysik, "Mobile Security: Threats and Best Practices ",

[8] A. K. Jha, S. Lee, and W. J. Lee, "Developer mistakes in writing android manifests: an empirical study of configuration errors," in Mining Software Repositories (MSR), 2017 IEEE/ACM 14th International Conference on, IEEE, 2017, pp. 25–36.

[9] Amy, "Help keep your android device safe - android help," [Online], Available: https://bit.ly/2DPTqa1, , 2018

[10] Ericsson Mobility Report, https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november2019.pdf, 2020.

[11] 75+ Mobile Marketing Statistics for 2020 and beyond, https://www.bluecorona.com/blog/mobile-marketing-statistics/, 2020

[12] 101 Mobile Marketing Statistics and Trends for 2020: https://quoracreative.com/article/mobile-marketing-statistics, 2020.

[13] Ryan Whitwan ," What is bootloader, and why does Verizon want them locked ?",ExtremeTech,2012

[14] Willam Stantan ," How to Check if Your Andriod Phone is Rooted",alphr ,2021

[15] https://www.alphr.com/check-android-phone-rooted/

[16] Alice MJ," Top 6 Andriod App Manager : Manage All Apps on your Andriod Device Effortlessly",Wondershare , Jan 2021

[17] Belal Amro ," Malware Detection Techniques For Mobile Devices",IJMNCT, Vol 7 ,Dec 2017.

[18] H.Patel,"14 best practices for your mobile app security," Tristate Technology , 2017, https://www.tristatetechnology.com/blog/best-practices-to-improve-mobile-app-security/.

[19] J.Callaham " The history of Android: The evolution of the biggest mobile OS in the world", Android Authority, May 2021.

[20] Kaur H, Ahamad S, Verma GN. Elements of Legacy Program Complexity. International Journal of Research in Engineering and Technology. 2015; 4(3):501-5.

[21] G. Narayanan, M. S. Ali and S. Ahamad, "Cyber secure consensus of discrete-time fractional-order multi-agent systems with distributed delayed control against attacks," 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2021, pp. 2191-2196, doi: 10.1109/SMC52423.2021.9658921.

[22] Abdul bari, Mohammed; Ahamad, Shahanawaj. (2011). Process of Reverse Engineering of Enterprise Information System Architecture. International Journal of Computer Science Issues. ISSN (Online): 1694-0814, Vol. 8, Issue 5, No 3, September 2011.