International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

A Review of Smartphone Security Challenges and Prevention

[1]Ogundele Israel Oludayo, [2]Akinwole Agnes Kikelomo, [3]Adebayo Adeniran Adedeji, [4]Aromolaran Adewale Ayodeji

[1,2,3,4]Computer Technology Department, Yaba College of Technology, Yaba, Lagos, Nigeria

***Abstract* - With the invention of a powerful, portable and lightweight device called a smartphone, there has been a very high number of its usage and a subsequent rise in the security issues involved in using a smartphone. Smartphones have gone from being non-existent many years ago to being heavily relied upon by a lot of people globally. This is because it is highly functional and contains various features. It is used for many different things like internet banking, entertainment, ecommerce, communication, mathematical calculations and many other things. Various types of smartphones and their distinct features were also identified, with android smartphone, iPhones, Window and Symbian being the top popular types of Mobile devices. Irrespective of the type of smartphone, there is a lot of data stored on it and most of the data stored are sensitive and susceptible to attack. There are a number of causes for smartphone security issues which can vary based on the type of the smartphone. Some of these causes were identified to be outdated OS or third-party apps, use of public WiFi, low security network protocols, physical breach and convergence. There are many examples of the security issues of smartphones which includes; malware attack, phishing attacks, spyware, identity theft, data invasion and theft and OS exploits. In the research work, we looked into ways to prevent these security issues which include; timely updates of OS and third-party apps, use of secure WiFi, use of antivirus, authentication and authentication. Desk research involving the literature review of "Smartphone" and "Smartphone security challenges and prevention" journals and articles were used. The research paper aimed to provide a concise knowledge and clear understanding of smartphones, its security and the prevention of the security challenges and also highlight the preventive measures that could be put in place to secure smartphones.**

Keywords: Smartphone, Security, Data protection, Vulnerability, Malware.

I. INTRODUCTION

Smartphone is a mobile device that enables its user to do more than calls and texts. It offers various functionalities which includes; working with an operating system, enabling users to browse the web [1]. It has the ability to contain application software just like a personal computer. There are numerous applications available to be downloaded on a smartphone for various personal and professional uses like; bank apps, games, health apps, social media platforms and many more apps. A smartphone is built to have a touch screen that enables the user to interact with the phone.

Smartphone devices are capable of performing a wide range of functions beyond just making and receiving phone calls. They typically come with a large touch screen display, a powerful processor to transform data and access to the internet via data network or Wi-Fi. It can also offer a wide range of features and functionalities, including email and messaging services, social media applications, cameras, GPS navigation, multimedia playback, and access to various mobile apps [2]; [3]. Many smartphones also come with biometric security features such as fingerprint sensors or facial recognition technology, as well as digital assistants like Siri or Google Assistant [4].

In 2021, there are over 3.8 billion smartphone users worldwide. This represents approximately 49% of the world's population, with smartphone usage continuing to grow rapidly in many regions. The number of smartphone users has steadily increased over the years, with the first smartphone has become an integral part of our daily lives, proving access to a wide range of functionalities [5]. The number of users is expected to continue to grow as smartphone technology improves and becomes more accessible in the global markets. With the relevance of a smartphone and the heavy reliance by the global population there have been some security concerns and problems due to the huge amount of data collected on a smartphone. In a report on mobile security published in 2021 by the security company check point, it was projected that four out of ten mobile phones are intrinsically vulnerable to cyber attacks [6]. The security challenges of smartphones are not just a projection, from the research carried out, it was discovered that threats to mobile security are increasing and more than 60% of digital fraud now occurs on mobile devices, from phishing scams to stolen credit card information. It was also discovered that the security challenge of a smartphone can vary based on the type of the smartphone [5].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

The security of smartphone devices is germane to the user to safeguard their information from malware attack. The measures taken to avoid or minimize the risks and threats that mobile devices face in terms of data privacy and security are regular software update, using biometric or strong password, avoid access untrusted site or downloading pirated software online, use VPN (Virtual Private Network) as your mobile security, do not use unknown Wi-Fi networks etc. The measures need to be taken to ensure security which is highlighted in this paper for users of smartphone to protect their data from unauthorized access or theft.

The main focus of this paper is to highlight the possible threats and vulnerability of smart phones, identify the four major operating system (Android, iOS, Windows and Symbian) of smartphone, to recognize the risk and challenges of using smart devices and to itemize the preventive measure of cyber security and best practices in using smartphone. The paper is organized as follows. In section (1) the research gives a background of smartphone security challenges, risk and preventive measures as objectives to the study. In section (2) the paper focus on the review of the smartphone in its use, challenges and risks. The section (3) was on prevention of the security challenges in using smartphone and best practices to improve security in ensure maximum safety and guard to detect malware attack. Section (4) concludes on the research with summary of the work.

II. REVIEW OF SMARTPHONE AND ITS CHALLENGES

Smartphones today are much more capable than mobile phones in terms of functionality. It now faces additional security threats as a result of its increased range of capabilities. Nowadays, a greater range of tasks are performed on phones, including online banking, social networking, shopping, and web application browsing. As a result, we must take precautions to keep our phones and sensitive information safe from assaults of all kinds. Always, an attacker goes after smartphones. They can attack through networks using Bluetooth and GSM services, as well as through communication channels like MMS (multimedia messaging services), SMS (short message services), and other channels. All of these take the form of harmful software that is unaware of all users. As a result, we must offer security at every level, including design, use, software development at the level of the operating system, and downloaded applications.

2.1 Operating System of Smartphone

Smartphone operating systems come in a variety. We discussed on the Android, iOS, Windows Phone, and Symbian operating systems in this section.

- **Android:** Android is a Google-developed open-source mobile operating system that is built on the Linux kernel. Four layers make up Android: the kernel, libraries, Android Runtime, and Application Framework. Application layer consists of all Android applications including email, SMS program, instant messaging, browsers, contacts and other various applications their names list is longer than few pages [7][8]. According to the authors in [9] and [10], application framework layer recognizes all Android applications. Android and the runtime library for Android make up the libraries layer. Dalvik and the Java Virtual Machine are combined in the Android runtime. Android's library is written in C/C++.
- **iOS:** The iOS is an operating system created by Apple Inc. for Apple devices. The iPhone, which debuted in 2007, is a prime example. Currently, one of the biggest rivals for smartphone market shares is the iPhone. Application of Apple phone will need computer running MAC OS [11]. Like Android, new iOS has been developed for third party to overcome the capability limitations of platform [12].
- **Windows Phone:** The Windows phone operating system was developed by Microsoft Corporation. Numerous devices, notably the HTC Titan and Nokia Lumia 800, were developed for this OS as of November 2011 [13]. After a year, Windows surpassed Android as the fourth most popular smartphone operating system. Windows adopts the security paradigm from the Android operating system.
- **Symbian:** Prior to Symbian, PSION was founded in 1980. Symbian was developed by Psion, Nokia, and Motorola in 1990 [14]. Following that, a few other suppliers, including Siemens and Sony Erickson, joined this company in 2002. The Ericsson R380 was the first mobile device to use the Symbian platform, which was soon followed by the release of a few Nokia N series models. C++ was used to design Symbian.

Nearly all smartphone operating systems offer ways for consumers to increase the security of their devices through specific login procedures. More than 30% of mobile phone users do not, however, utilize their PINs. On the other hand, the amount of high valued contents stored on the phone is rapidly increasing, with mobile payment and money transfer application as well as enterprise data becoming available on mobile devices [15].

2.2 Smartphone and Uses

Users have been enabled and encouraged by the mobile revolution to migrate nearly all of their daily activities into the mobile environment via so-called mobile applications. As a result, both the user and developer communities for mobile

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

devices are experiencing significant growth. Mobile devices are treated by their users as very personal tools, mainly used to facilitate everyday operations, but they also serve to store very sensitive personal information [16]. Smartphone devices is widely used and accepted globally to carry out business transaction and also for communication, irrespective of your age or education background.

2.2.1 Types of Smart Phone

There are different types of smartphones and the popular ones can be found in the table 1 below:

Table 1: Smartphone Brand and features

S/N	Brand	Operating System	Features
1	Apple	iOS	FaceTime, Freeform, Game Center, iCloud+, Inclusive Language, Lockdown Mode, Apple Watch mirroring, etc.
2	Samsung, Redmi, Pixel, Sony etc.	Android OS	Messaging, Autocorrection and Dictionary, Web browser, Voice-based features, Multi-touch, Screen capture, Multiple language support etc.
3	Nokia	Windows OS	Multimedia, Text input, Web browser, Contacts, Email, Search, Games, etc.
4	Amazon's Fire	Original Fire OS	Dynamic Perspective, Widgets, Facial Recognition, One-Handed Shortcuts, Firefly, etc.

2.2.2 Uses of Smart Phone

Irrespective of the type of smartphone, there are many uses of a smartphone and some of the popular uses by individuals include the following:

- Communication: Smartphones have bridged the gap between people in different places through phone calls, text messages, and video calls. It is used as a medium for both professional and personal means of communication. They utilize communication channels like WhatsApp messenger, emails, Facebook messenger, WeChat, etc.
- Social media: In recent times, social media has become hugely popular among young and old people, and smartphones have made it easy for users to keep up with others and share their experiences and ideas while they're on the go. People use Twitter, Instagram, and Facebook frequently throughout the day because they can express themselves while still feeling connected [17].
- Gambling: A significant portion of the enormous online betting market is conducted on smartphones. Almost anything can be gambled on, and in recent years, online virtual sports betting has gained popularity as a fun way to kill time wherever you are, as a social activity to engage in with friends and a way to make quick cash [17].
- Media (photos and videos): Smartphones have audio and video components that enable individuals to take videos and pictures with them. It also enables the individual to store and share these media files.
- Music: Rather than the use of CD or DVDs to access and play music files, music can now be played on a smartphone making it easy to be entertained on the go.
- Finance: With the advance of technology, financial institutions are moving with the trends and taking their business online. With a smartphone, financial transactions can be made on the go at any place making payments easy and feasible anywhere.
- Ecommerce: Commercial activities are carried out online with the use of smartphones. People can buy and sell things online and access these ecommerce websites through the use of a smartphone.

2.3 Smartphones Cyber Security Risks

The European Union Agency for Network and Information Security (ENISA), acting also as regional advisory body for Asia [18] identified the top six risks for the smartphone users [19].

- Data leakage Resulting from Device Loss or Theft: Data leakage can have a severe impact as 97% of smartphone users according to the Kaspersky global survey [20] store a combination of self-created photos/videos/music, personal email, SMS, passwords/PIN codes, phone contacts, banking details. Users are particularly vulnerable if they don't use any form of authentication on their device.
- Unintentional Disclosure of Data: This has to do with mobile applications getting too much access to phone content so they can reveal data online or to the developer. Data disclosure can also occur when using open Wi-Fi hotspots to transmit data without encryption.
- Attacks on Decommissioned Phones: Due to advancements in digital forensic tools, data can now be

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

recovered from phones that have undergone a factory reset before being sold again, discarded, or handed to a facility that decommissions mobile phones. After a factory reset, it is typically advised that the user upload phony data and carry out another factory reset. The likelihood of finding the original data is substantially decreased if the technique is repeated numerous times.

- Phishing Attacks: User credentials, such as passwords or credit card data, are collected by an attacker utilizing phony applications, SMS, or email messages that appear to be legitimate. Users of smartphones may be at risk if they are unable to recognize phishing emails, SMS messages, or counterfeit online links that request passwords or other sensitive information.
- Spyware Attacks: By downloading and installing programs from unreliable sources, malicious software (also known as malware) that have the ability to record, steal, and transfer data to their developers, the attacker, may wind up on a smartphone. Threats typically originate from unofficial app marketplaces. However, spyware can occasionally be covered up by programs from the Apple Store or Google Play.
- Network Spoofing Attacks: This frequently occurs in open-access Wi-Fi hotspot settings, where an attacker creates a Wi-Fi with a name that might look legitimate in order to watch the information that users connecting to it send and receive. Such operations can be carried out on even trustworthy open Wi-Fi networks. When these networks are password-protected, the password is frequently accessible or quickly guessable.

2.4 Mobile Device Security Issues

This is the problem that arises the most frequently in mobile cloud computing as a result of theft or loss of the mobile device. Here, the user's data represents the primary loss. Any mobile device that an attacker gains access to will have data and applications used without authorization. The device can also be used to do some unwanted tasks like botnet: to carry out DoS or DDoS attack through mobile device [21]. A new attack related to power consumption is carried out on mobile devices when the device is connected to the wireless network; then its power consumption increases to discharge device battery fast [22]. The security of a user's personal data is compromised when it is synced to the cloud from an internal storage location on a mobile device while using mobile cloud computing. Malware and viruses are among the most traditional forms of attack in mobile computing, yet they are still powerful and still function on mobile devices because the mobile operating system isn't reliable or safe.

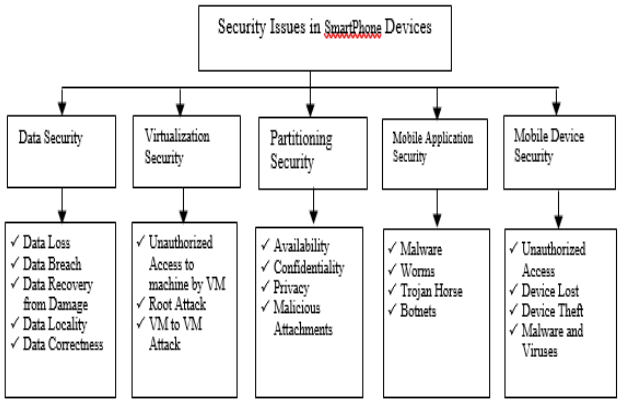

Figure 1: Smartphone security issues

- Data security: The technique of protecting digital data from unauthorized access, unintentional loss, disclosure, alteration, manipulation, or corruption throughout all stages of its life—from creation to destruction—is known as data security. The confidentiality, integrity, and availability of an organization's data must be protected through the use of this procedure. Data must be kept confidential, have integrity to ensure it is accurate and reliable, and be available for authorized parties to access.
- Virtualization Security: The term "virtualized security," sometimes known as "security virtualization," describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls.
- Partitioning Security: In the persistent storage memory of the device, partitions are logical storage units created. By using partitioning, you can logically divide the available space into parts that can be accessed separately from one another. Mobile devices will inevitably hold both personal and professional data. Partitioning the data on your device is strongly advised to improve the security of both personal and corporate information. If you need to delete the data, separating the data makes the procedure easier.
- Mobile application security: By using mobile app security, you can protect your digital identity and high-value mobile applications from fraud in all of its forms. This covers tampering, reverse engineering, malware, keyloggers, and other types of interference or manipulation. A thorough mobile app security strategy incorporates technology options like mobile app shielding as well as industry best practices and internal company procedures.
- Mobile device security: Mobile device security refers to the safeguards put in place to guard sensitive data

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

transmitted and stored on computers, smartphones, tablets, wearables, and other portable devices.

2.5 Smartphone Malware and Attack

Smartphones can be attached by malware through installation of programs and downloading of content from the internet. These programs can perform some illegal act on your mobile devices thereby causing some damage or destruction to important content of the user. The smartphone malware can be put into three; (i) mobile malware (ii) Infection channels of malware and (iii) Black industry chain of malware.

A) Mobile malware

Mobile malware refers to software that is downloaded to a smartphone, runs, and does illicit tasks, such as stealing a subscriber's private information or deducting money from their account without their consent or prompting. Malware has some characteristics which including: Mandatory installation; Difficult to uninstall; Browser infection and Gathering user privacy information.

At present, there are five common malwares, namely virus, worm, Trojan, botnet, and spyware.

- Virus: Smartphone operating systems can become infected by viruses, which are self-replicating programs that propagate from one smartphone to another. The data on a subscriber's phone is intended to be deleted or altered.
- Worm: Worm is a harmful, self-replicating application that has been extensively disseminated yet may not affect a smartphone's system files. Worms primarily function to take up system and network resources.
- Trojan: Trojan is a malicious program that poses as legitimate software and, after being installed on a user's computer, carries out various destructive actions without the user's knowledge, such as backdoor Trojans that frequently include keyboard recorders, spy Trojans that steal user accounts, etc.
- Botnet: A botnet is a program that an attacker can use to command a large number of smartphones that have zombie apps installed to carry out harmful actions simultaneously, such as DDOS attacks on specific websites or the mass texting of spam to specified recipients.
- Spyware: Spyware is a computer application that can gather user data from mobile phones and distribute it to a third party without the user's knowledge or consent. As an illustration, this application tracks the keystrokes made on a mobile device and gathers private user data, including the IMSI and IMEI, a password, a credit card number, and a personal identification code. Additionally, it harvests email addresses and monitors a user's browsing habits.

B) Infection channels of malware

According to the 2011 NetQin mobile security report [23], approximately 79% infected smartphone users download malicious software by the network, 13.6% of them were infected by sending SMS/MMS, 4.2% of them through Bluetooth, 3.2% of them via a memory card or other transmission ways. It has been determined that mobile internet and WAP are crucial infection channels, and SMS and MMS are additional crucial channels. Therefore, in order to significantly lower the infection rate, it must concentrate on tackling the malware issue via networks and SMS/MMS.

C) Black industry chain of malware

Behind the mobile malware outbreaks, a black industry chain is hidden which consists of the following roles.

- Employers: A criminal organization, a bad SP, or a CP tries to forcefully convey their business information to the user.
- Channel agent: It is accountable for all aspects of suggested scheme, information dissemination, and company promotion.
- Hackers: It assumes responsibility for providing technical assistance for malware, such as creating malicious code, managing botnets, sending spam texts, or assaulting specific people as required by employers. Black industry chain has two work modes:
- Mode 1: Added value SP and smartphone manufacturers cooperate to install built-in malicious programs before handset selling. Users buy and use these infected mobile phones without any awareness.
- Mode 2: Criminal group and SP distribute the malicious software on internet, and hacker controls the infected smartphone, stealing user private information, sending spam messages or doing any illegal actions.

2.6 Security in Android, iOS, Windows and Symbian

In both Android and iOS smartphones, the security challenges can be classified into the following four categories:

- Physical: Due to their portable and lightweight build, smartphones are more susceptible to loss or theft when compared to computers. When a hacker gets physical access to a stolen or lost smartphone, the hacker may flash a device with a malicious system image that connects to a computer to install malicious software or carry out data extraction [24].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

- Network-based: Common wireless network interfaces like Wi-Fi and Bluetooth are used by mobile devices to connect to the internet. Each of these interfaces is vulnerable to wireless eavesdropping efforts using widely accessible software like Wifite or Aircrack-ng Suite and has its own intrinsic weaknesses [25].
- System-based: Smartphone manufacturers may unintentionally embed a vulnerability into the device while producing it. The "No iOS Zone" vulnerability is one illustration; it automatically connects any iOS devices nearby to a fake network and frequently crashes the device to prevent its use [26], [27]. A later version of iOS ultimately contained a fix for this vulnerability [24].
- Application-based: Third-party programs on smartphones could be a source of security threats. These apps may be outdated and made vulnerable to security attacks. Some software developers either neglect to distribute software updates on schedule or stop supporting outdated OS versions. Users could not immediately update programs on their mobile devices, even if software upgrades are available. The likelihood that an attacker may use vulnerabilities included in out-of-date software increases [24].

2.6.1 Security Challenges in Android

It's open-source nature, business model and play store management makes it very susceptible to security attacks. Timely updates of android OS and the OS version compatibility with hardware also affect the security of the android device [28]. Since Android is an open-source operating system, several different customized versions of it are used on numerous devices. Support and security employees may have a difficult time in managing the security because of this situation. Big companies like Google are striving to make timely OS updates to smartphones and Samsung are incorporating their own security; Knox security technology to combat and reduce security challenges in their smartphones.

2.6.2 Security Challenges in iPhones

The security is different in iPhones compared to android due to its closed ecosystem. The iPhone operating system is managed by Apple and they tightly control the applications that are installed on an iPhone. Apps that work on iPhones are specifically designed and developed for the iPhone operating system. This control of their ecosystem enables the smartphones to have tight security, because its ecosystem has fewer touch points than platforms with hardware-OS fragmentation, Apple is better equipped to maintain each of its products and guarantee security for a longer length of time. Due to Apple's more compact framework, even older phones might still be able to run the most recent OS and apps and gain access to all the most recent security upgrades. The closed environment only allows applications that don't access the phone's source code, which lessens the need for iOS antivirus and makes it impossible to develop an iOS antivirus for App Store approval [29].

Despite the security provided by iPhones, the smartphones are not 100% secure from attacks. They are still susceptible to security challenges but it is minimal in comparison to android smartphones. For example, Malware attacks are not immune to iOS. If Apple misses any security gaps or chooses to implement some undesirable security measures, there will be very little to no control over these virus attacks. Also, an iPhone can be physically breached when it is lost or stolen but there are measures put in place to combat and reduce the security breach. Features like find my iPhone can be used to set a passcode and lock the phone if it was not set previously to prevent access to sensitive information. It also enables the owner to remotely delete the phone's data to prevent leak of sensitive information [30].

2.6.3 Security Challenges in windows

Windows smartphones, although less prevalent compared to other mobile operating system like android and iOS, still face certain challenges such as malware and viruses, lack of updates, application security, phishing attacks, data leakage and weak authentication etc. To address these security challenges, users of Windows smartphones should take several precautions to be mindful of their online activities and practice good security hygiene to protect their devices and data [31].

2.6.4 Security Challenges in Symbian

Symbian is an outdated operating system that was once widely used in smartphone, but it is no longer supported by Nokia and other manufacturers [32], [33]. However, it may still be present in some legacy devices. Some of the challenges are lack of updates of the application, malware attack, weak authentication, data leakage etc. users of Symbian should be mindful to take preventive measures to secure their mobile device. However, given that Symbian is no longer a supported operating system, it is not recommended to continue using it as it is likely to be extreme vulnerable to security threats [34].

2.7 Causes of Smartphone Security Challenges

Aside from the causes of smartphone security challenges that were discussed earlier for iPhones and Android phones, there are some root causes of security challenges which are listed below:

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

- Convergence: Smartphones are both physical and network assets and this is the main cause of the numerous mobile security concerns. Boundaries that have been put in place for security can be compromised. A mobile device, for instance, can be out of your physical control but yet connected to your internal servers and company data. It can also happen vice versa, when someone inside your building could be using a smartphone that is connected to harmful external network resources [35].
- Physical Breaches: A smartphone can be physically breached when a phone is stolen or lost and a hacker gets hold of the device. With a device in hand rather than online, password cracking and other breach methods are considerably easier to carry out. Consumer smartphones don't have enough security measures in place to fend off a determined attacker. Particularly PIN codes are infamously simple to decipher [35].
- Out-of-Date Hardware: Smartphone manufacturers stop issuing stability and security updates after a specific amount of time, just like with computer operating systems. Older BYOD (Bring your own device) devices that are being used may come under attack when hackers discover a new vulnerability in outdated mobile software [35].
- Targeted Attacks: Phishing campaigns, ransomware, and data-harvesting assaults are just a few examples of the network attacks that can target mobile devices and their users. Although these assaults are mostly not specific to mobile devices, hackers are increasingly using them to target them.

III. PREVENTION OF SECUIRYY CHALLENGES IN SMARTPHONES

[36] Have given a technique for authentication of the user by using biometric features. This method uses biometrics to identify authorized and unauthorized users by analyzing patterns created by a user's hand movement while holding a mobile device. In [37] authors discussed Google device policy application. This application is very much useful when the mobile device is stolen or lost user can clean his data online and also enables device token (unique key) which ensures the notification security. [38] Have given the approach of OpenFlow in which OpenFlow switch is integrated with mobile to do the job of redirection, while communication of mobile and all cloud data is passed through OpenFlow, so that the data are secure while being transmitted. Let's consider the preventive measure of the smartphone from various vulnerabilities that exist in using the devices.

A) Prevention of security challenges in Android

- Ensure installed apps are from trusted sources: to prevent malicious attack via apps, a user should ensure that the apps they want to install are from trusted sources and not shady sources.
- Close attention to permissions asked by an application that the user wants to install.
- Frequent updates of android OS.
- Avoid clicking unnecessary ads because the advertiser's site may secretly install a Trojan or backdoor on the android device.

B) Prevention of security challenges in iPhone

- Don't jailbreak an iPhone device: To ensure an iPhone gets the protection it has from its closed system; owners should not jailbreak an iPhone to access apps or software that are not available in the Apple ecosystem.
- Frequent update of iOS: timely updates of iOS enable the device to have access to improvements in security features and new fixes in previously overlooked weak points.
- Timely updates of apple id security: with a user's apple id, a user's security can be compromised if the apple id can be accessed hence the need for timely update of password security.
- Avoid connecting to public or untrusted Wi-Fi: if a user connects to a public Wi-Fi, it makes it easy for hackers to get access to their smartphones and break their security.

C) Prevention of security challenges in window

- Keep the operating system up-to-date
- Download Apps from trusted sources
- Use strong authentication methods
- Install antivirus and security software
- Avoid insure Wi-Fi networks
- Implement remote tracking and wiping capabilities
- Practice good hygiene

D) Prevention of security challenges in Symbian

- Limit app download
- Keep software updated
- Use strong authentication
- Be cautious of phishing attempts
- Backup and secure your data
- Practice safe web browsing
- Consider device replacement

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 5, pp 234-245, May-2023

https://doi.org/10.47001/IRJIET/2023.705030

E) General Prevention of Security Challenges in Smartphone

To combat the smartphone security issues, there are various methods to employ and they include the following:

- Use mobile device management software and access control on any smartphone connected to your network.
- Create network security software for desktop and mobile platforms to track down and stop data from leaving the network.
- Pass policies that enable data loss prevention (DLP) procedures.
- Only allow authorized employees to access and use business devices.
- Perform routine checks on smartphones and install app updates.
- Enforce privacy protection from third party apps.
- Avoid leaving smartphones unattended.
- Use smartphone authentication and encryption.
- Users should only connect to reliable networks using WPA21 or better network security protocols.
- Execute timely mobile device updates.
- Use an antivirus.
- The download and installation of apps should be subject to restrictions.
- Continuously learn about current mobile device attacks and vulnerabilities.
- Avoid using public Wi-Fi.
- Ensure regular backup of data and make sure it is secure.

3.1 Improving Smartphone Security Features

Three of the most desired security characteristics of a smartphone are confidentiality, integrity, and authentication. The majority of cellphones enable PC and device synchronization. Another user will be able to access the file system on the smartphone thanks to this feature. Therefore, users should utilize encryption methods and refrain from keeping sensitive information in plaintext on a smartphone in order to keep data private. Integrity pertains to both the system and the data. In order to prevent unauthorized modification, app retailers should check software integration. Additionally, cellphones should include safeguards to maintain system integrity. They must also reject requests for unlawful access to data. Users of smartphones could be shielded from malware assaults that fake caller IDs and MMS by using a smartphone authentication service. Because femtocells increase capacity and coverage, authentication is crucial to confirm a carrier's legitimacy. However, there are some easy ways to improve smartphone security:

- Raising awareness about security. A smartphone can be hacked, infected, or phished just like a laptop or desktop computer. When downloading software19 or allowing it access to flash memory or smartphone sensors, users of smartphones should be aware of potential dangers and assaults. Add a password and set the device to automatically lock after a while. These safety measures are supported by the majority of cellphones.
- Don't keep irreplaceable information on your smartphone. Smartphones are prone to theft and loss.
- Regularly create smartphone backups. Connect your smartphone to a computer, and make sure to regularly backup your data.
- Bluetooth should be turned off when not in use. Your smartphone can catch viruses using Bluetooth.
- Do not connect to the Internet using unsecured Wi-Fi hotspots. Smartphone data traffic can reveal vital information to packet sniffer software like Wireshark.
- Use a reputable and dependable security tool to protect your smartphone.
- Inquire with the smartphone manufacturer or service provider about antitheft features like "erase data" or "default smartphone" from a distance.

3.2 ITU and NSA Security Requirements for Smartphone

International Telecommunication Union (ITU) and US National Security Agency [39], [40] have defined and laid down certain generalized security requirements of mobile cloud computing. They are as follows:

- Confidentiality: The fact that data from mobile users is processed on a public network and kept on a public server makes confidentiality a crucial necessity. As a result, there is a good probability that data belonging to mobile users would be accessed improperly. As a result, mobile cloud service providers have a lot of confidentiality challenges.
- Availability: Availability means cloud service is always available for users 24/7when they need the service. There are various attacks that affect availability, but mobile cloud computing service providers need to prevent them and always ensure the service is available for mobile users.
- Authentication and Access Control: This entails recognizing the legitimate user of the system using certain login patterns or any other type of authentication technique. Access control is the process of authenticating users of the system before granting them access to restricted resources so they can complete certain tasks. Access control governs all user actions, including reading, writing, updating, wiping data, etc.
- Integrity: Integrity is the avoidance of data loss or change while it is being transmitted across a public

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 234-245, May-2023
https://doi.org/10.47001/IRJIET/2023.705030

network. Integrity is concerned with the accuracy and consistency of user data.

- Privacy: Confidentiality, integrity, and authentication are used to secure the personal data of mobile users while communicating in the cloud.

3.3 Best Practices for Smartphone Security

Mobile security best practices are recommended guidelines and safeguards for protecting mobile devices and users' data [41]. In general, hardware and software vendors outline and promote procedures and instructions which, properly applied, should maintain or increase the security level. Although there is no way to 100 percent guarantee security, as unforeseen vulnerabilities can be discovered and exploited by attackers, let us take a look at some recently developed best practices for mobile devices and applications [42–46].

- Make user authentication the highest priority: most mobile devices can be locked with a screen lock and unlocked with a password, biometric (e.g., fingerprint and face recognition) or personal identification number (PIN) [47]. Nowadays, multifactor authentication is considered as the best practice to protect user's data [48]. On the contrary, security is entirely based on password complexity and the user's attention to its confidentiality.
- Update mobile operating systems and on-board applications with security 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 [49].
- Back up user data on a regular basis: backing up is a basic method of preventing data loss or deletion. A backup schedule should be adapted to an increase in data over time. Examples of user data include individual user files (documents and spreadsheets), media files (e.g., pictures and videos), contacts, and other sensitive data [50]. The obvious solution for mobile devices is a remote backup, which entails copying and storing files in a personal or public cloud. However, in this instance, transmission speed is the key issue.
- Utilize encryption: Data encryption converts information into a different format, or code, making it possible for only authorized parties to decrypt and view the information. Data transmission across the network and data storage on mobile devices both use encryption features. However, encryption by default needs a password to both encrypt and decode data files. When a password is forgotten, data recovery is frequently difficult and unsuccessful. Instead, relying solely on publicly accessible solutions could just mislead a user into believing they are absolutely secure. Moreover, it is also strongly advised not to connect to and use a public and insecure Wi-Fi spot without using a secure transmission option such as a virtual private network (VPN) [51].
- Enable remote data wipe: in case a user has their device with sensitive data stolen and there is little chance of retrieving them in a relatively short period of time, one should consider turning on the device capability which allows a factory reset message to be remotely executed [49, 50]. Furthermore, remote data wiping is essential in the event of work termination or the acquisition of virus that cannot be removed or uninstalled. The current technologies are not a panacea for mobile security, despite their undeniable benefits.
- Disable Bluetooth and Wi-Fi when not needed: minimizing both Bluetooth and Wi-Fi usage reduces exposure to having vulnerabilities exploited, although the flaws are not in these standards, but in their implementations [52]. It should be noted that in this case, a user must intentionally interact with the system before it may be disabled. However, there are programs (such as Auto- Bluetooth) that, in accordance with the rules set by a user, automatically turn Bluetooth on or off.
- Be aware of social engineering techniques: social engineering is a term that encompasses a broad spectrum of malicious activity such as phishing, pretexting, baiting, quid pro quo, and tailgating ("piggybacking"). With this human-centric focus in mind, it is up to a user to be aware of malicious "actors" who engage in social engineering attacks hunting for human greed and ignorance [48, 52].
- Be sure not to jailbreak your device: The goal of jail breaking is to remove software limitations put in place by the device's manufacturer. In other words, applying a sequence of kernel patches enables root access, which enables the installation of apps that are not provided through the app store. Jail breaking can seriously expose an operating system to additional vulnerabilities, effectively exploited by attackers [56, 53]. One should also keep in mind that, in case of removing manufacturer restrictions, the device's warranty will most likely be voided. Moreover, a decrease of overall system stability might occur since buggy apps tend to utilize substantial amounts of hardware resources.
- Be sure not to grant unnecessary permissions to applications: The privileges an app has, such as the ability to access the camera, contact list, or location, are known as app permissions. Depending on the vendor, current operating system versions come in a range of flavors. One key principle is to only allow permissions

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 234-245, May-2023
https://doi.org/10.47001/IRJIET/2023.705030

that are required for the program to function as intended. In other words, a user should always employ the principle of least privilege (PoLP) [54].

- Install mobile security and antivirus applications: Mobile security and antivirus real-time scanners protect against dangerous programs, viruses, identity theft, ransomware, and cryptominers because there is no additional security by default. Moreover, some tools can also scan URLs and block dangerous sites, monitor links in text messages, and provide parental control [56, 57].

IV. CONCLUSION

With the resourcefulness, creativity and innovation of humans, a very useful and powerful device; a smartphone was developed. Despite its usefulness, it could be a two-edged sword and be dangerous when it is vulnerable to attacks. With the increase in smartphone popularity, there is also an increase in its attacks. From this paper various types of mobile devices were identified with iPhone, Window and Symbian and android being the most popular. Security challenges in iPhone, Android, Window and Symbian were identified along with the causes, examples and prevention of security issues. From the discussion of the security stance of iPhone and Android, it can be deduced that in terms of security, iPhone offers its users more security and is less prone to security challenges compared to android smartphones. Although there are preventive measures that can be put in place to combat and reduce security challenges of smartphone irrespective of the type cannot be 100% secured, it can only be protected to some extent and the chances, severity and frequency of the attacks can be greatly reduced.

REFERENCES

[1] M. Sarwar and T. R. Soomro, "Impact of smartphone's on society," Eur. J. Sci. Res., vol. 98, no. 2, pp. 216–226, 2013.

[2] D. Singh Negi, "Using mobile technologies in libraries and information centers," Libr. hi tech news, vol. 31, no. 5, pp. 14–16, 2014.

[3] O. O. Okediran, O. T. Arulogun, R. A. Ganiyu, and C. A. Oyeleye, "Mobile operating systems and application development platforms: A survey," Int. J. Adv. Netw. Appl., vol. 6, no. 1, p. 2195, 2014.

[4] M. Z. Iqbal and A. G. Campbell, "From luxury to necessity: Progress of touchless interaction technology," Technol. Soc., vol. 67, p. 101796, 2021.

[5] P. T. Mai and A. Tick, "Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam," Acta Polytech. Hungarica, vol. 18, no. 8, pp. 67–89, 2021.

[6] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in iot-based cloud computing: A comprehensive survey," Electronics, vol. 11, no. 1, p. 16, 2022.

[7] M. Ahmad and N. Musa, "Comparison between android and iOS Operating System in terms of security," in Information Technology in Asia (CITA), 2013 8th International Conference on. IEEE, 2013, pp. 1–4.

[8] M. Goadrich and M. Rogers, "Smart smartphone development: iOS versus Android," in Proceedings of the 42nd ACM technical symposium on Computer science education. ACM, 2011, pp. 607–612.

[9] L. Ma, L. Gu, and J. Wang, "Research and Development of Mobile Application for Android Platform," Int. J. Multimed. Ubiquitous Eng., vol. 9, no. 4, pp. 187–198, 2014.

[10] J. Liu and J. Yu, "Research on Development of Android Applications," in Fourth International Conference on Intelligent Networks and Intelligent Systems. IEEE, 2011, pp. 69–72.

[11] T. Grønli and J. Hansen, "Mobile application platform heterogeneity: Android vs Windows Phone vs iOS vs Firefox OS," in Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on. IEEE, 2014, pp. 635–641.

[12] D. Tilson, C. Sørensen, and K. Lyytinen, "Change and control paradoxes in mobile infrastructure innovation: the Android and iOS mobile operating systems cases," in System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, 2012, pp. 1324–1333.

[13] V. Remenar, S. Husnjak, and D. Peraković, "Research of Security Threats in the Use of Modern Terminal Devices," in 23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability, 2012.

[14] A.Maji and K. Hao, "Characterizing failures in mobile oses: A case study with android and symbian," in Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on. IEEE, 2010, pp. 249–258.

[15] O. Riva and C. Qin, "Progressive Authentication: Deciding When to Authenticate on Mobile Phones.," in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)., 2012, pp. 301–316.

[16] P. Weichbroth and Ł. Łysik, "Mobile security: Threats and best practices," Mob. Inf. Syst., vol. 2020, pp. 1–15, 2020.

[17] C. Shane-Simpson, A. Manago, N. Gaggi, and K. Gillespie-Lynch, "Why do college students prefer

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 234-245, May-2023
https://doi.org/10.47001/IRJIET/2023.705030

Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital," Comput. Human Behav., vol. 86, pp. 276–288, 2018.

[18] ENISA: Critical Applications – Smartphone Security Top Ten Risks. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-tenrisks. May 2016.

[19] Kaspersky Lab: One in every six users suffers loss or theft of mobile devices, 21 October 2013. http://www.kaspersky.com/about/news/press/2013/one-in-every-six-users-suffer-lossor-theft-of-mobile-devices. July 2016.

[20] Denscombe, M.: The Good Guide Research Guide for Small-Scale Social Research Projects, 4th edn. Open University Press, Maidenhead (2010).

[21] L. Liu, X. Zhang, G. Yan, S. Chen, in Exploitation and Threat Analysis of Open Mobile Devices. Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems (2009), pp. 20–29.

[22] R. Racic, D. Ma,H. Chen, ExploitingMMSvulnerabilities to stealthily exhaustmobile phone's battery. Securecomm Workshops 2006, 1–10 (2006).

[23] N. Q. Mobile, "Mobile Security Report." 2011.

[24] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," Inf. Sci. (Ny)., vol. 421, pp. 43–69, 2017.

[25] E. F. E. Ahmet and M. B. KAPLAN, "Wi-fi security analysis for E&M-Government applications," Int. J. Multidiscip. Stud. Innov. Technol., vol. 3, no. 2, pp. 86–98, 2019.

[26] H. Susanto, "Revealing cyber threat of smart mobile devices within digital ecosystem: User information security awareness," in Data Integrity and Quality, IntechOpen, 2021.

[27] M.-L. Yao, M.-C. Chuang, and C.-C. Hsu, "Research on the User Attitudes and Behaviors of Mobile Security and Antivirus.".

[28] S. Garg and N. Baliyan, "Comparative analysis of Android and iOS from security viewpoint," Comput. Sci. Rev., vol. 40, p. 100372, 2021.

[29] B. Remneland-Wikhamn, J. A. N. Ljungberg, M. Bergquist, and J. Kuschel, "Open innovation, generativity and the supplier as peer: The case of iphone and android," Int. J. Innov. Manag., vol. 15, no. 01, pp. 205–230, 2011.

[30] M. Talal et al., "Comprehensive review and analysis of anti-malware apps for smartphones," Telecommun. Syst., vol. 72, pp. 285–337, 2019.

[31] A.Das and H. U. Khan, "Security behaviors of smartphone users," Inf. Comput. Secur., vol. 24, no. 1, pp. 116–134, 2016.

[32] G. Jindal and M. Jain, "A comparative study of mobile phone's operating systems," Int. J. Comput. Appl. Inf. Technol., vol. 1, no. 3, pp. 10–15, 2012.

[33] M. Nosrati, R. Karimi, and H. A. Hasanvand, "Mobile computing: principles, devices and operating systems," World Appl. Program., vol. 2, no. 7, pp. 399–408, 2012.

[34] J. West and D. Wood, "Evolving an open ecosystem: The rise and fall of the Symbian platform," in Collaboration and competition in business ecosystems, Emerald Group Publishing Limited, 2014.

[35] T. Pitichat, "Smartphones in the workplace: Changing organizational behavior, transforming the future," LUX A J. Transdiscipl. Writ. Res. from Claremont Grad. Univ., vol. 3, no. 1, p. 13, 2013.

[36] Z. Sitová, J. Šeďenka, Q. Yang, G. Peng, G. Zhou, P. Gasti et al., HMOG: new behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Inf. Forensics Secur. 11, 877–892 (2016).

[37] R. Neware, K. Ulabhaje, G. Karemore, H. Lokhande, and V. Dandige, "Survey on Security Issues in Mobile Cloud Computing and Preventive Measures," in Smart Computing Paradigms: New Progresses and Challenges: Proceedings of ICACNI 2018, Volume 2, 2020, pp. 89–100.

[38] V. Moorthy, R. Venkataraman, and T. R. Rao, "Security and privacy attacks during data communication in software defined mobile clouds," Comput. Commun., vol. 153, pp. 515–526, 2020.

[39] Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications (2016), https://www.itu.int/itudoc/itu-t/85097.pdf

[40] US National Security Agency: Information Assurance (2016), http://www.nsa.gov/ia/ia_at_nsa/index.shtml.online

[41] Webopedia, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.

[42] F. Stroud, "Mobile security best practices," 2020, https://www.webopedia.com/TERM/M/mobile_security_best_practices.html.

[43] H. Dowden, "-e 6 mobile device security best practices you should know in 2020," 2020,

ISSN (online): 2581-3048
Volume 7, Issue 5, pp 234-245, May-2023
https://doi.org/10.47001/IRJIET/2023.705030

https://www.ntiva.com/blog/top-5-mobile-device-security-best-practices-2020.

[44] D. Hein, "7 essential mobile security best practices for businesses," 2020, https://solutionsreview.com/mobiledevice-management/7-essential-mobile-security-best-practicesfor-businesses/.

[45] S. Lerner, "Mobile device security best practices. How to protect portable technology," 2020, https://www.Enterprisemobilityexchange.com/eme-security/articles/mobiledevice- security.

[46] J. Mark, "8 best practices for mobile device security," 2020, https://www.jmark.com/8-best-practices-mobiledevice-security/.

[47] A.D. Kent, L. M. Liebrock, and J. C. Neil, "Authentication graphs: analyzing user behavior within an enterprise network," Computers & Security, vol. 48, pp. 150–166, 2015.

[48] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," in Advances in User Authentication, pp. 1 85–233, Springer, Cham, Switzerland, 2017.

[49] H. Patel, "14 best practices for your mobile app security," 2020, https://www.tristatetechnology.com/blog/bestpractices-to-improve-mobile-app-security/.

[50] M. Ciampa, Security Awareness: Applying Practical Security in Your World, Cengage Learning, Boston, MA, USA, 2013.

[51] K. Lab, "Best practices. Encryption," 2020, https://media. kaspersky.com/pdf/b2b/Encryption_Best_Practice_Guide_2015.pdf.

[52] L. Phifer, "Best practices for improving mobile data security," 2020, https://searchmobilecomputing.techtarget.com/tip/Best-practices-for-improving-mobile-data-security.

[53] A.S. K. Pathan, M. M. Monowar, and Z. M. Fadlullah, Building Next-Generation Converged Networks: Deory and Practice, CRC Press, Boca Raton, FL, USA, 2013.

[54] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: trends, tactics, and implications," Technology in Society, vol. 32, no. 3, pp. 183–196, 2010.

[55] D. Burley, R. Carpinella, D. Chesebrough et al., Cybersecurity in our Digital Lives, Vol. 2, Hudson Whitman/ECP, New York, NY, USA, 2015.

[56] V. K. Velu, Mobile Application Penetration Testing, Packt Publishing Ltd., Birmingham, UK, 2016.

[57] M. E. Vermaat, S. L. Sebok, S. M. Freund, J. T. Campbell, and M. Frydenberg, Discovering Computers 2018: Digital Technology, Data, and Devices, Nelson Education, Toronto, Canada, 2017.

Citation of this Article:

Ogundele Israel Oludayo, Akinwole Agnes Kikelomo, Adebayo Adeniran Adedeji, Aromolaran Adewale Ayodeji, "A Review of Smartphone Security Challenges and Prevention" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 5, pp 234-245, May 2023. https://doi.org/10.47001/IRJIET/2023.705030

****

