Cybersecurity and digital forensics year 3

Module: individual project

Supervisor: Mrinal Sharma

Student ID: M00729531

Chapter 2 literature review

Table of Contents

Acknowledgement:

First and foremost, I thank the almighty God for guiding me through the entirety of this research project. I thank my supervisor and his help in the accomplishment of this research study. Some shortcomings occurred in the process of this study. However, giving up was not an option which contributed to the strength that was needed to complete the research project.

IOT security flaws and mitigations.

Topic focus: security vulnerabilities in Samsung smartphones.

1. Introduction

in today's world, smartphone devices are more than just devices for calling or texting. They hold a big chunk part of our lives, from memory images saved in the device's gallery to personal information such as banking information. One of the most popular phones used in the world is Samsung A12, which runs an android operating system with an android 12th version. Android version 12 in one of recent latest version which was released in 2021 and it was expected that the version 12 would enhance safety features and prevent any breaches or intrusion from threat actors. However, vulnerabilities keep arising due to the popularity of the android OS and vulnerabilities can still be exploited and data privacy can be compromised.

The Samsung A12 model provide good chances to dive into security issues that are found in android systems. according to the Mirror, there been several

Samsung devices that have been exploited due to its security flaws and hackers could remotely attack the devices *(Snelling, 2023)*. The popularity of Samsung devices can help examine and understand so much about phone safety. This research study will be focusing on uncovering the safety issues of the Samsung A12 smartphone and what steps can be made to further strengthened the devices safety. By a close investigative measure at the Samsung smartphone, the hope is to accumulate information and understanding that will help later mitigate the security issues of Samsung devices.

The importance of this research project is enormous reports of data breaches, data loss that the main issues in sourced withing smartphones. It is not just a problem on the reputation of manufacturer of the smartphones, but the burden is transferred to all that uses a smartphone. By exploring the Samsung A12 device, the aim is to expose the common security issues that many might face when using the smartphone and measures that could be taken to counter such security issues.

The reason to specifically investigate the Samsung A12 device depended on several factors including the price of the smartphone, which is affordable by many users by just 7,000Rs in Mauritius *(Samsung galaxy a12 red, no date)*. It is user-friendly due its operating system and we also considered the popularity of Samsung devices. Due to the considerable factors, Samsung smartphones would be an excellent to study and specifically vulnerabilities that are present in the A12 model.

The review is set up to delve deep into smartphone potential security issues. It is set to start by studying the background of smartphone security and how it evolved overtime. The research shall proceed by discussing specific problems and security risks issues in the Samsung A12 smartphone and existing study reports that shall provide a wider understanding of the cause of the security issues and comparing ways that have been used to fix the issues found in the smartphone. This research study shall critically evaluate the smartphone's related security issues and suggest new solutions to make the Samsung smartphone safer for users.

The following sections, we shall explore and explain the points made in detail. The aim of this research is to further the conversation on security issues found in Samsung devices by exploring and pinpointing the where the issue lies and mitigating those issues for a safer world for data.

2. Background:

In the last two decades, the evolution of smartphone security has defined the explosive growth and integration of these devices into our daily lives. The early stages of modern mobile phones were primarily used for calling and texting. However, the arrival of smartphones has made a transformation into people lives that impacted both in a positive way because of the multitask ability of a smartphone and negative way due to the security issues that come along with an unsecured smartphone. The integration of smartphones into people lives have brought a myriad of tasks from browsing and GPS navigation to managing finances such e-payment and controlling smart home devices such as modern Tv's. The evolution of smartphones has not just brought merit to the world but created a central issue since smartphone have now been an integral part of our daily lives. Some of the issues include privacy concerns, data security and national security too.

2.1 The early days of the smartphone revolution

The early days of the smartphone revolution, mobile phones had minimal security features often with limited security features as the first mobile phones with security features such as PIN numbers in the year of 2000's. company's such as Nokia produced the first mobile phones with security features such as PIN numbers to unlock the phone. As smartphones emerged, integrating OS such as Android, the importance of security grew as the OS became more sophisticated. Android was created in 2003 and developed by Android Inc and which later was bought by the Google company. Following the acquisition of the operating system by Google, android became a leading operating system in the world in smartphones by a market value of 70.69% while other competing operating systems such as IOS have hold only 28.58% *(Iphone vs. Android user & revenue statistics (2024), 2024)*. Some of the merit that

are attributable to the android OS is that it allows customization, innovation and can host third party software applications without some much restriction out on it. Independent developers enjoy its open-source model which is favorable to rapid innovation. However, its openness or open-source model sets ground for vulnerabilities and increased potential risks of malicious software to intrude the smartphone OS and open the door to data breaches.

2.2 Android response to emerging security issues

Security issues have long been recognized in an android operating system in various android version. Google has extensively enhanced the security of each android version. Some of the most enhanced features that have been applied to android OS's include app sandbox that is a Linux user -based protection that identifies and isolates app resources *(Android security features, no date)*. Sandbox helps in code execution and runs it in an isolated area to not affect any other apps or the OS. Google play protect is another crucial feature that Google added, which test and scans apps especially from third party developers to determine whether the apps have malware or malicious behavior coded in them. However, vulnerabilities have been consistently becoming persistent to each version of android and sometimes due to the ecosystem of android. Most partly because updates might be not consistent in all devices in the android ecosystem.

2.3 Samsung and Android 12

Samsung is one of the biggest manufacturers of various products that include Tv's (Television), fridges, washing machines and smartphones. Samsung is the largest manufacturer of android devices in the world and with that position as being the biggest manufacturer of android device, Samsung has played a significant role in structing the security of its devices. The Samsung company developed its own security platform named Knox. Knox provides various security features that aimed at securing sensitive information against unauthorized access and illegal tempering of data. the introduction of the android version 12 on devices such as the Samsung A12, represents the various effort made by the Samsung company to strengthen security in their devices with some features that bring transparency in the inner working of the

devices and providing control over the devices in aspects such as data and app permissions.

2.4 Emerging threats and solutions

as technological advances are being made, so are the methods used by cyber criminal activity becoming more and more sophisticated. Threats such as ransomware attacks, phishing attacks and unsecured WIFI networks remain as the main threats of the modern-day world that is making advances in digitalization and handling most of our data on cloud systems. However, solutions that counter the threats that arises each time have seen progress as more sophisticated solutions are being made available such as biometric authentication methods, facial authentication solutions, fingerprint recognition and end-end data encryption. the latest security enhancement methods being applied is with AI (artificial intelligence) which can help in anomaly detection systems and mitigate threats in real-time.

2.5 The importance of constant vigilance

It is crucially important to learn and be knowledgeable on the history of smartphone security and the technological emerging threats. The security hygiene from understanding how various threats is very important to users as we investigate the security features of the Samsung A12 and their flaws and hope the security flaws in future Samsung android version can be avoided. Some of the crucial solutions include regular updates, reviewing app permissions and being vigilant on phishing attempts on private user data.

As we moved from the early simplistic mobile phones with minimal security features to mobile phones that are highly capable of multitasking and handle large amounts of data, have had a notable highly significant security advancement. However, the increased sophisticated threats that emerge everyday due to the vulnerabilities in many Samsung smartphones, users must remain extra vigilant about the sensitive data that they might be holding in the mobile phones as more and more personal data Is entrusted to be handle by smartphones and the stakes remain high.

2.6 Relevance of the project

This project study has the potential to shed light on the security flaws of Samsung devices as well as security flaws in the android operating system. Samsung, being one of the popular smartphones has stayed in the conversation of mobile security vulnerabilities that are emerging in mobile devices including Samsung too. This project has the potential to improve the security of Samsung devices by evaluating areas often ignored by developers that can be the backdoor for threat actors.

3. Problem description:

3.1 Understanding the security vulnerabilities in Samsung smartphones

Smartphones such as the Samsung A12 have an integral part in an everyday user's experience and daily lives, not just as communication devices but also as data handling tools that can handle various types of user data. the role that been given to smartphones to be able to handle any type of user data are subject to various security threats. User data in smartphones is prone to security risks depending on the vulnerabilities that can be exploited in android devices such as the Samsung A12 [12] [19].

3.2 Common threats to smartphones security

3.2.1 Unsecured network connection:

The use of unsecured network connections such as WIFI network connections can be a risk to user's personal user data due to the likelihood of data to be intercepted. According to Kaspersky, three British politicians took part in a security experiment that aimed to demonstrate how an unsecured network can be a security threat to user's data and all three politicians were easily hacked and their social media, PayPal data and VoIP conversations were able to be intercepted and their data were exposed *(Top 7 mobile security threats, 2023)*. The goal was reached of the experiment which had the aim to emphasize the risk that unsecured network presents and why to avoid such unsecured network connections [34].

3.2.2 Malware and viruses:

These are harmful pieces of code that if injected in the smartphones, can potentially damage the phone, steal sensitive user data, and can perform other various such as mobile phone control. These malicious pieces of code can mainly be found in App stores such as Google Play that host third party software applications. Google has a security measure in place that scans the Google play protect that scans Apps looking for malware or malicious behavior in Apps [35]. However, some apps may be developed to appear as safe and may deceive the security check put in place and be able to go unnoticed. Other forms of malware may come in the form of phishing email or unsecured websites. Once the malware is installed on the devices, users can be subject to theft and ransomware *(Top 7 mobile security threats, 2023)* [34].

3.2.3 Weak encryption methods:

Weak cryptography methods for encrypting user data are a huge security issue that many smartphones face. Developers sometimes build apps and use weak or known encryption that may be subject to security attacks due to its weakness in a securing user data and further ignore the recommended encryption up-to-date standards, so that they speed up the development process of Apps [42]. The results to such negligence, the attackers job becomes easier if they are familiar with the weak encryption applied to the application and can easily obtain crucial information such as passwords.

3.2.4 Phishing attacks and social engineering:

These kinds of attacks are increasingly used by attackers to trap users and surrender their personal information. Furthermore, such attacks come in various forms such as emails, text messages that may look as if it is from a credible source. For Samsung users, the integration of personal and work accounts on their smartphones may potentially be a vulnerable spot of such phishing attacks [34] [36].

3.2.5 App permissions:

App permission is a very crucial aspect of modern mobile phones. Many apps request more user permissions than what is necessary for their

overall function. The overreach of such app permission request can lead to potential disclosure of personal information [56]. Mismanagement of app permission can be critical to user data in a mobile smartphone.

3.3 Android security cast study: Samsung A12

The Samsung A12 that has an android version 12, has both strong and weak smartphone security. The android 12 include enhanced security features such as app permissions, location permissions and biometrics authentication [4]. However, the device's specific security features implemented by Samsung may play a role in some security outcomes since the Samsung company may apply its own set of security features. Some of the vulnerabilities may include issues like its bootloader that may require regular updates to address emerging security threats.

3.4 The wide range implications of security breaches

The implications of security breaches or vulnerabilities are very deep. A security breach in a smartphone device can potentially lead to various scenarios that include identity theft, unauthorized access of financial information and unauthorized purchases. Furthermore, implications can become broader when IoT devices in an ecosystem can wider the security threat to data and serve as entry points for threat actors and leading to network breaches and data breaches *(What mobile security threats pose a risk to your organisation?, 2023)*.

3.5 Mitigation measures and best practices:

Preventative measures to counter the risks of security breaches, manufactures and users should be vigilant of all type of security known risks. Smartphone manufacturers such as Samsung must provide users with option that can help prevent common security incidents. Regular updates, flagging apps that seems to have malicious behavior from the google play store, ensuring communication has an end-to-end encryption and utilizations of common basic security features such as biometrics locks [9].

Understanding and mitigating security vulnerabilities in smartphones in the modern day age where smartphones are becoming increasingly an integral

part of users lives and professional life due to functionalities and help perform some basics task in advance to save time and it is the understanding of such potential issues that may arise and harm our personal information has become critical due to security threats that are discovered and threat actors await to exploits the vulnerabilities presents in smartphones such as the Samsung A12.

4. Sources and impacts of security vulnerabilities in Samsung smartphones.

4.1 Sources of security vulnerabilities

the causes of security vulnerabilities In Samsung smartphones can originate from various factors. Recognizing and understanding the causes of security vulnerabilities in smartphones such as Samsung is crucial to help mitigate the risks and prevent threats to user data.

4.1.1 User behavior:

Often users are required to use the strongest password including lower cases and upper-case letters plus special characters such as “@, #” to further strengthen the password and making it harder to hackers and other malicious apps that may attempt to crack the password or other various methods used to steal passwords such as phishing and eavesdropping attacks. Such kind of attack occur on unsecured network connection that can be used to intercept communication between two devices to modify, steal user data [57].

4.1.2 Third-party software applications:

Third part apps present a significant potential risk to user data in smartphones. According to the New York post, smartphones user was warned to delete or not attempt to install or use 17 flagged finance apps that were infected with malware *(Archive and feed, 2024)*. It is disguised as a legitimate financial application which was a trojan horse which was prone to steal personal sensitive information from users.

4.1.3 System software flaws:

Some of the operating systems components can be subject to cyber-attacks when the component has system flaws inherently embedded in them from the different manufacturers. Smartphones such as the Samsung A12 can have different hardware or system component manufactured by other manufacturers that are not Samsung and can affect the devices. Considering, android ecosystem poses a significant threat due to fragmentation where different devices are running android with different versions *(Kelly, 2023)*.
The delay in security patches or reinforcement in android ecosystems aggravates these vulnerabilities in the Samsung smartphones that run android systems [57].

4.1.4 Hardware components:

Hardware components are not excluded from the security issues that arises in modern day smartphones. Hardware components can have security flaws embedded in them. Issues in chipset have shown to be exploited by attackers to gain access to the smartphone device. As According to the WION publication, Google was able to make discoveries of 18 vulnerabilities in the Samsung Exynos chipsets and warned users about using the devices with the Exynos chipset *(Pathak , 2023)*. Security vulnerabilities can arise in all aspects of the device and moving forward mitigations of such issues is crucial by starting on the production line and evaluation each part of a smartphone before assembly.

4.1.5 Other related causes of vulnerabilities in Samsung smartphones:

These vulnerabilities are caused by improper app permissions in the android operating system. Security vulnerabilities such as improper access control whereby attackers can access and read information stored in SD card and if information stored in SD card can be accessed by other apps in the smartphone according to the latest CVE-2024-20847, which a vulnerability documentation and the vulnerability detail is about Samsung vulnerabilities [57].

4.2 Impacts of security vulnerabilities

4.2.1 Financial fraud and identity theft:

Financial fraud and identity are the most common forms impact that the results of the security vulnerabilities that are exploited in smartphones by attackers. The user data stolen is used in various illegal activities such as ransom blackmailing, were attackers use data stolen as hostage and request a large sum of payment. Furthermore, user data might be used to illicitly make illegal purchases online and attackers might be able to open new accounts and obtain loans in someone's else name. the two-factor authentication method is another layer of security that has been applied to combat such attempts by attackers.

4.2.2 Loss of privacy:

There is a significant loss of privacy when user data is exposed by hackers. Loss of privacy can sometimes lead to reputational damage, lack of privacy over communication between two users, lack of privacy when the user's location is disclosed and sometimes some vulnerabilities can be so severe on the privacy of the user when components such as the smartphone camera and microphone can be accessed without the user's permission or knowledge. As reported by Reuters, sometimes the vulnerabilities can be exploited on a massive scale like the exposure made by the security analyst Edward Snowden, who exposed the mass surveillance that was being done by the US (united states) on its citizen where they could tap and monitor calls or listen to conversations through the phone microphone *(Satter, 2020)*.

4.2.3 Legal implications:

Organizations or companies can face legal challenges if they fail, or user data is lost or misused under their control. There have been several fines imposed on many organizations for failing to secure properly user data and resulting in a data leak. Samsung is not new to such fines, where they were fined almost 900 million for a series of data leaks between the year 2020 and 2021 *(Nam, 2023).* The incidents involved a mishandling of user data over the Samsung cloud where users could upload videos and images as one of the services and the vulnerability in that service was hit by a cyber-attack and a breach occurred [22]. The fine comes with other GDPR (General data protection regulation) fines imposed on different organizations such as meta and amazon.

4.2.4 Data manipulation:

Some of the most impactful that could occur to user data after breach or access involve data modification. Once attackers have access to user data, modification of user data Is highly probable for various purposes that the attacker intent to use the modified information [34].

4.2.5 Denial of service (Dos):

This is a common impact from vulnerabilities present in Samsung devices and across the board like in windows operating systems *(Dash, 2023)*. An attacker could remotely exploit vulnerabilities in Samsung devices and cause a denial of service to users [34].

5. Existing research and solutions

5.1 Current existing research

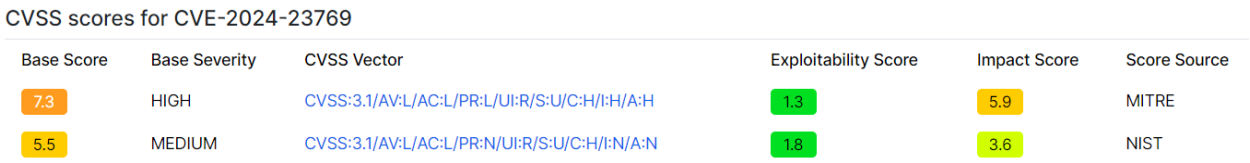
Research into smartphone security has increased on a notable high pace due to the critical part smartphones play in user daily lives, current existing research aims to provide current and past findings regarding vulnerabilities and attacks methods performed by attackers and along with new developing strategies to minimize the impacts of vulnerabilities regarding mitigations of future risks that arise from vulnerabilities.

5.1.1 User behavior research:

It is crucial to understand how users use these smartphones devices which would help to understand how certain security threats are able to occur so easily. Often users use simple passwords and do not regularly update their devices to the latest updates available. It can be understandable that some updates can pass unnoticed or just refuse to update their devices willingly or unknowingly. Through a survey that looked at many organizations to find that, if most employees or the organization use updated version whether on their personal mobile devices or personal computers. Remarkably, half of the organization surveyed confirmed that they still use outdated technology and 62% of those organizations had employees still using outdated technology on their mobile devices, which is a significant number [38]. Such behavior can escalate the attacks coming from cybercriminals, if they happen to be lucky to find out an organization still uses outdated technology.

5.1.2 Vulnerability assessments:

Researchers constantly explore android operating systems and regularly documents the findings on popular platforms such as CVE (common vulnerability and exposure) details, which sheds light on vulnerabilities found in many technologies including Samsung devices. CVE documents findings of vulnerabilities in technologies including mobile android devices as well Samsung devices since they have an android operating system [37]. CVE classifies the vulnerabilities in a scoring list from less severe to highly severe.


CVSS scores for CVE-2024-23769

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	1.3	5.9	MITRE
5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N	1.8	3.6	NIST

Figure 1: CVE vulnerability details.

As shown in figure 1, It shows the scoring of a certain vulnerability with the name CVE-2024-23769 which is like a numbering for vulnerabilities since they are many of them and the researchers may determine the severity and impact of the vulnerability found, where some

vulnerabilities may have a high score and other a medium score, a negligible score or critical score.

Severity	Base Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 2:CVE score board

The score board aims to document the severity of the vulnerability found and users may need to avoid such vulnerabilities due to the severity of the impact such a vulnerability can cause if security measures aren't applied like regular updates to get rid of unwanted vulnerabilities [37].

5.1.3 Malware analysis:

Another crucial focus is malware analysis of malware attacks that target android systems especially android systems in mobile devices. There are several regular research findings often publish by security companies that document how malware affect modern day smart devices including most popular operating system android. Computer security firms have often documented the ways malware is downloaded in the device and other ways the malware can stealth itself in the device without triggering any alarms or suspicions from the user, most referred

to as trojans *(McAfee, 2022)*. The researchers also point out ways a user may check out signs of a malware presence on device with factors such as:

- Longer load time of applications:
  Applications on the phones may take longer to start than usual.
- Unlimited ads.
- Applications the user never downloaded may appear.
- Battery drainage
- The OS of the phone has significantly slowed down.

According to HT tech news, one of the big discoveries on android phones made by researchers was a malware that disguised itself as a system update and could go unnoticed by users or even security experts *(Tech, 2022)*. The malware performed a range of illegal activities including taking control of the smartphone, accessing personal private messages such WhatsApp texts, accessing images, and stealing the images, can record and listen to conversations, access GPS (Global positioning system) location of a user and take photos too [32]. Such discoveries are very important into learning the sophistication of new malware and how best to detect such malware.

5.2 Security solutions to enhance smartphone devices.

Responses or security solutions for unlimited vulnerabilities that do not seize to come up with the advancement of technology has been a fore front for researchers and developers regarding android smartphones. Solutions include technical and behavioral solutions to counter the risks of those vulnerabilities being exploited by attackers.

- Software updates and patch management:
  One of the most common defenses that are mostly basic is regular software updates for android OS. Samsung has regular security updates for various of its devices which some are updates are available every month and other have yearly updates for different devices. The security updates include the Samsung A12, it has a biannual security update *(Samsung mobile security, no date)*. Simply meaning the Samsung A12 smartphones has security updates twice a year [27].
- Advanced security features:

Samsung continues to apply effort to enhance the security of its devices. A great example is the Samsung Knox which is a preinstalled security software that provides services to protect sensitive data safe (*Samsung Knox security principles for protection | Samsung Levant*, no date). One of the method Knox uses to protect sensitive data such as PIN (personal identification number), Samsung Knox has an isolated secured storage that is encrypted and handles and stores highly sensitive data [20]. provides an isolated execution environment for sensitive software that handles sensitive user data such as user payment method or a user making a purchase, all run in a secured controlled execution environment. Furthermore, Samsung Knox also applied intrusion detection services that may alter the user if an intrusion is detected from a potential threat or malicious application. Lastly, Samsung Knox has a highly strict security process that covers the entire lifespan of the product or in this case the mobile phone in order and provides the user with the latest security updates and security patches to combat various attacks.

- Education and awareness:
  There are several programs ran by Samsung and Google to educate and raise awareness on potential security threats and active mobile threats that users face daily and how it can be prevented as well as how users can combat when face with mobile threats such as malware. Cybersecurity has an awareness month which is celebrated every October and technology companies such as Samsung and Google use the opportunity to raise awareness on the best practices that user can use to ensure the most sensitive data stays safe [11]. The 2023 cybersecurity month campaign, Google encouraged raised awareness on Some of best practices in cybersecurity that include the use of stronger password protection, the use to multifactor authentication (MFA) and regular updates *(Hansen, 2023).* on the other hand, in the same moth of last year 2023, Samsung not only participated in the awareness campaign but had also developed some security solutions to provide Samsung users with the latest security features that include the Samsung wallet that enabled users to be able to make contactless

payments while using any of their products in their ecosystem that include smartwatches or smartphones [40].

- Security Collaboration:
  Cybersecurity collaboration is another important aspect of combatting threats faced on android systems and at large. Technology companies and security firms and governments often partner to enhance security solutions and share knowledge on current and potential threats *(Schalla, 2023)*. Throughout years, there are several forums that take place as the CyberRisk CISO dinner, the event involves cybersecurity experts that get together to share experiences and knowledge on cyber threats and ways to develop robust security solutions [51].

6. Comparative analysis: Samsung smartphones and other smartphones brands.

comparative framework overview:

smartphone security comparison involves several key aspects that include its operating system security features, the manufacturer security enhancements, the frequency and prominence of security updates. Lastly, how the security updates really translate into real-world security against threat attacks.

6.1 Operating system security: Android vs other operating systems

- Android security (Samsung A12):
  Samsung smartphones including the Samsung A12, use android as its operating system and it is considered an open-source code OS due to flexibility that can allow to user to customize it. However, being open source is a risk to potentially be vulnerable to cyberthreats. Samsung has developed its own security measures with the known security platform named Samsung Knox that is preinstalled in all their smartphones [20]. The Samsung Knox adds several security layers like secure execution environment, encrypted data storage and real-time monitoring.
- IOS security (iPhone 7 smartphone):
  IOS is the operating system for Apple products and operates on a closed system. Closed source means its source code is not accessible to

users or be customized by users and is closely guarded by the manufacturer of the operating system which is the Apple company. IOS has a strict app evaluation before accepting any app on their app store. Furthermore, an app to be approved into the app store of iPhone or any apple product, a thorough examination is conducted on the developer's app and the developers are also identified by apple to evaluate whether have any suspicious history or a known hacker [41]. The identification of app developers is done in form of a subscription, developers must register and be given authorization to upload their application on apple app store platform and well after their app have been vetted to be legit and contain no malware. IOS has additional layers of security that vets the developer's app after transferring or uploading it on the app store and basically checks for any modification done before the app is uploaded on the app store which would be suspicious activity worth to check [41]. Apple ensures that all devices receive the regular updates simultaneously to minimize the risk of any vulnerabilities being discovered and exploited by attackers.

6.2 Manufacturer specific security enhancements (Samsung vs Google Pixel)

- Samsung Knox:
  The Samsung Knox reinforces the overall security of the device from the chipset level upwards ensuring a low risk level of unauthorized access to the user data [26]. The Samsung Knox operates on a multi-layered security level that can isolate certain processes for execution in a secure environment and uses an encryption level of AES256-XTS for sector-based storage [42].
- Google Pixel security features:
  The google pixel security features has some similarities on the way Samsung Knox operates because it is still an android smartphone. However, the only main differentiative aspect is that google pixel uses a security chip named the Titan M security chip [44]. The security chip provides an additional on top of the android's default security measures already in place *(Wankhede, 2024)*. The chip has its own memory, RAM and disk encryption which are designed to house the most sensitive user

information such as biometrics, PIN and decryption keys and protected from malicious apps to access such data. isolated security environment has been an answer in preventing unauthorized access to user data from malicious apps or hackers and other brands adopting the methods such as the Apple M1 chip that has a hardened security measures such as the locking feature that prevents hackers from reactivating the device or formatting the device in scenario where the device is stolen [46].

6.3 Frequency and effectiveness of security updates

- Samsung updates:
  As Samsung ecosystem is growing, Samsung has committed itself to ensure regular updates for all its devices including the Samsung A12 that has its biannual regular updates which are scheduled twice a year [27]. Samsung commitment to regular updates is very crucial to keep their customer base happy to not draw them closer to its competitors such as the Apple company, which it is its biggest rival in smartphone market even though android users make up 70 % of smartphone market share [10].
- Other manufacturers (Huawei and Xiaomi):
  Other smartphone manufacturers such as Huawei and Xiaomi, security updates may vary sometimes based on the region of user or device which would delay security updates to be applied in time. For devices such as Xiaomi, security updates may take up to 4 to 5 years for models that came after the Xiaomi 13T, which is a great risk for potential vulnerabilities that cannot be fixed in time or regularly [47]. Whereas Huawei promises monthly and quarterly security updates and specific models, some devices receive regular security updates every month and other devices may have to wait 3 months for security patch updates [47]. The decentralization in android ecosystem is a significant security risk due to the delays of security patch updates reaching all android devices.

6.4 Real-world protection against threats (Samsung and other brands):

- Effectiveness in preventing attacks:
  Android systems may be vulnerable to attack due to its open-source characteristics. However, the Samsung Knox security system in Samsung devices including the A12, have shown effectiveness in countering potential risks to user data caused by malware and system vulnerabilities [20]. It is also crucial to note that, no operating system is entirely immune to security breaches such as malware and other attacks that may compromised user data and Samsung devices have had some significant high level security breaches In the past such as the malware discovered disguised as a system update and had the power to record conversation, access images in the phone's gallery, access private text messages and could listen to phone calls [32].
- Comparison of attack prevention effectiveness with other smartphone brands (iPhone):
  Taking iPhone as example, within the mainstream or one most popular smartphone, iPhone is more secure than android systems overall due to its strict management of devices in its ecosystem thus having less malware incidents reported in contrast to android *(Markuson, 2024)*. Furthermore, Apple provides the iPhone with faster security updates and for a longer term, Apple has lesser devices in ecosystem which helps in management than android which has a large range of devices, that explains why android is the most targeted than IOS [48].

6.5 User experience and security management (Samsung and Apple):

- Samsung:
  Samsung provides a well balance option to users regarding security and usability. Samsung users can manage and customize their security settings extensively to boost or make the user experience more enjoyable to users. Samsung has a customization service which can boost the user experience by using user's data and using the data in various ways such as product recommendation such as music based on information collected about the user and their music taste [49]. The customization service based on information collected about the user, it

can provide or recommend customized information based on the user's information. However, If the settings are managed badly, more information can be collected about the user than necessary, which is a potential risk to user data theft.

- Apple:
  Apple is more restrictive on what it can allow user to manage or control and especially offering users customization services. Apple provides less customization services options than any other smartphone regarding security settings customization [50]. However, offers more controlled environments and overall provides a significantly high security level.

7. Critical analysis of Samsung A12 security

7.1 Evaluation of Samsung's security framework

Samsung has regularly employed robust security frameworks, particularly the implementation of the Samsung Knox, which is installed on all devices including the Samsung A12 to mitigate or counter the emerging mobile threats [20]. The Samsung Knox security framework provides data encryption, real-time protection when it comes to detecting anomalies whether from malicious apps or malicious activities, secure boot to prevent unauthorized bootloaders [52]. However, the security measures may be robust on paper but their true effectiveness in the real world when faced with threats can vary based on the various factors such as user behavior and implementation.

7.2 Strength of Samsung security

Samsung's security framework begins at the hardware level which is crucial to maintain hardware integrity via the Knox security platform. Essentially, the Samsung's Knox platform ensures the hardware of the mobile device's integrity is maintained from the startup of the device to ensure sensitive data is well protected fully. Regular updates have been part of the commitment Samsung has made to its users. Due to the emerging vulnerabilities in different android versions, it is necessary to provide regular updates to users to address the security flaws in time and helps the user experience being conveniently trustworthy knowing the device is secure against emerging

mobile threats. Furthermore, Samsung has added another security layer that is also employed by other manufacturers of smartphones which is biometric security. Devices such as the Samsung A12 have the security feature which uses fingerprint scanning to provide access to the rightful owner of the device. The biometric security feature complements the other security layers provided by the Samsung Knox security platform to enhance access control and user authentication.

7.3 Weakness and areas for improvement

Due to the emerging threat that smartphone devices face, the android ecosystem may come as the key suspect to the reason why android systems may be an easy target to threat actors. Fragmentation in android systems has posed a significant security issue because Samsung's devices may not receive security patches and updates consistently. The inconsistency or the delay in regular security updates on all devices can leave the door open to the exploitation of vulnerabilities. In contrast to other smartphone brands such as the iPhone, Apple has a much better advantage on android phones simply because no other phone uses the IOS operating system and security vulnerabilities are addresses only solely based on the iPhone devices. Android is available on many devices which makes it harder for Google to address all security vulnerabilities on all devices using android as its operating system. The model of the device is a crucial aspect of the security updates that are given by Google, a device such as the Samsung A12 which received security updates only twice a year is also a security vulnerability itself due to how old or less popular the device may be, leaving the device vulnerable for a long time [54].

Third-party applications pose an issue on android devices including Samsung devices which uses the Google play store and Google has more flexibility on third-party software apps that other closed and controlled app environment such as the apple store which is tightly controlled and strictly screened to mitigate the distribution of malicious apps *(Goad, 2023).* The android system open nature to third-party applications to end-users poses a high risk to user data due to how easy end-users can install third-party apps and the openness

nature of android invites all sorts of sophisticated malicious apps posing as legitimate software thus potentially compromising sensitive user information.

The complexity and user experience of the security features in android phones including the A12 makes complicated for users or average users from managing their security settings even though the security features are beneficial to the average user. The complex security settings in android devices may lead to misconfiguration of lack of the know-how in terms of navigating though security settings that may benefit the user's data protection. At times, the average user may fall short on gaining the knowledge of the security settings and utilizing the security features. According the ScienceDirect, mobile apps are becoming more complex and hence making the user experience more complex too *(Corral, 2021)* [55]. Users may ignore the security settings or features that are designed for the user's benefit and potentially risk being compromised by vulnerabilities that may arise depending on the version of the android system.

A comparative form of view displays how the clear contrast between different mobile industries whereby one industry may give flexible measures where users can manage their own security settings and other industries have a more controlled ecosystem and uniform levels of security which allows less customization options to users. Samsung has an open security approach by allowing users to customize their own security settings, be able to install third-party apps with less restrictive measures or apps that are not typically in the app store such as Google play store. The Apple company that produces the iPhone has a more controlled environment to provide a high of level security to user's information and restrict on any unvetted third-party applications thus leaving the end-users with less customization options. However, Samsung complex security settings could be made more flexible with user interface that is simplified for users to manage efficiently their security settings. Furthermore, Samsung could expand on its investment and make more educational campaigns that may inform users arising mobile threats and best practices to counter or avoid the emerging mobile threats. Lastly, Samsung can learn from other brands such as Apple on how a controlled user environment can benefit the overall security of their

smartphones against malicious apps that many times come from third parties.

8. Summary of findings

8.1 Key findings on security features and vulnerabilities

8.1.1 Operating systems security:

As discussed throughout the existing research, Samsung smartphones use android as it's operating system. The openness of android provides flexibility and customization to users but android being open source comes with huge security threat. However, Samsung has developed security measures to counter the various security issues that android systems face by developing the security platform Knox. Knox provides essential security features such as real-time monitoring, secure boot and data storage encryption. a comparison insight discussed how other operating system such as IOS have a uniform or closed security measure that allows less customization from the user and has a strict vetting for third-party applications before they are distributed in its app store unlike like Samsung that uses android and android has less restriction on third party apps being installed on their devices.

8.1.2 Manufacturer security system's enhancements:

Different aspects of security from different mobile devices manufactures were discussed including the Samsung Knox security platform and Google Pixel security chip. Both security systems have shown to have similarities in their way of working such as isolation of sensitive user information, hardware-level security and incorporate biometrics and encryption for a higher level of security. However, slight differences are shown by different manufactures such as the use of security chip used by Google to isolate user information such as biometrics and encryption keys.

8.1.3 Security updates:

Security updates between different mobile manufacturers have shown commitment between two mobile manufacturers Samsung and Apple.

Samsung has shown to have regular security updates for different devices and the timeline for the security updates for different devices. In the research, the focus is more on the Samsung A12 and comparing it to its competitor the iPhone. A biannual security update is addressed to a set of Samsung devices including the Samsung A12 security vulnerabilities. The frequency in the security updates timeliness of Samsung devices in contrast to Apple devices such as the iPhone has shown unequal distribution of security updates on Samsung devices and an equal distribution of security updates of Apple devices across its ecosystem.

8.1.4 Real-time threat protection:

Threat protection in Samsung devices appear to need more robust security improvements in the future due to the openness of the android operating system even though Samsung's own security measures such as the Samsung Knox platform have shown strength in countering emerging sophisticated mobile threats especially coming from malicious mobile software applications that sometimes can disguise itself as a legitimate app. Other companies such as Apple which have a unique closed operating system have demonstrated themselves to be more secure with very few breaches unlike its competitors such as Samsung.

8.1.5 User experience and management:

Samsung offers a user-friendly experience when it comes to their devices and provides customization options and management to its users. However, mismanagement is an occurrence with many users due to different factors such as lack of knowledge on certain security features and mismanagement can be a potential security vulnerability that can lead to security breaches. A comparison insight between Samsung and Apple has shown that a restrictive operating system that allows less customization to users and security features managed by the manufacturer are more less to be a target to threat actors. Apple's approach is more restrictive than Samsung, which manages most of the security features and provides necessary customization to users.

8.2 Areas of improvement:

- User education:
  More efforts must be made in educating users on the management of security features and best practices to ensure there is a minimal risk of breaches that may be associated with poor management.
- Security Update frequency and distribution:
  An increased frequency of security across Samsung's ecosystem can enhance overall smartphone security against emerging threats. some Samsung phones such as the A12 tend to be not a high priority to manufacturers and prioritize the latest Samsung phone or the most sold ones. Affordable Samsung phones such as the A12 which get security updates twice a year can benefit from an increased frequency update each month.

9. Expected findings:

This research will investigate in search of vulnerabilities in the Samsung A12 device. This research will attempt to find new vulnerabilities with the android version 12 and how affected the device potentially was or has been. the aftermath of the investigation and analysis of the vulnerabilities, this research shall propose the best possible mitigations measures that can be applied to other related Samsung mobile devices.

10. References:

[1] A. R, “Data Manipulation: Attacks and Mitigation – CSIAC.” Accessed: Jun. 30, 2024. [Online]. Available: https://csiac.org/articles/data-manipulation-attacks-and-mitigation/

[2] A. N, “The Android Ecosystem: Your Gateway to a World of Connected Devices and Smart Living.” Accessed: Jun. 30, 2024. [Online]. Available: https://www.linkedin.com/pulse/android-ecosystem-your-gateway-world-connected-devices-nasir-abas-81qpf

[3] “Android | Definition, History, & Facts | Britannica.” Accessed: Jun. 30, 2024. [Online]. Available: https://www.britannica.com/technology/Android-operating-system

[4] “Android 12,” Android Developers. Accessed: Jun. 30, 2024. [Online]. Available: https://developer.android.com/about/versions/12

[5] “Android 12,” Android. Accessed: Jun. 30, 2024. [Online]. Available: https://www.android.com/android-12/

[6] “Android Security Features,” Android Open Source Project. Accessed: Jun. 30, 2024. [Online]. Available: https://source.android.com/docs/security/features

[7] V. A. Archive and G. author R. feed, “Smartphone users warned to delete these 17 dangerous apps.” Accessed: Jun. 30, 2024. [Online]. Available: https://nypost.com/2024/01/02/tech/smartphone-users-warned-to-delete-these-17-dangerous-apps/

[8] C. J, “Smartphone history: the timeline of a modern marvel.” Accessed: Dec. 31, 2023. [Online]. Available: https://blog.textedly.com/smartphone-history-when-were-smartphones-invented

[9] M. Concannon, “The 7 Mobile Device Security Best Practices You Should Know for 2024.” Accessed: Jun. 30, 2024. [Online]. Available: https://www.ntiva.com/blog/top-7-mobile-device-security-best-practices

[10] “Global Smartphone Market Share: Quarterly,” Counterpoint. Accessed: Jun. 30, 2024. [Online]. Available: https://www.counterpointresearch.com/insights/global-smartphone-share/

[11] “Cybersecurity Awareness Month,” *NIST*, Sep. 2016, Accessed: Jun. 30, 2024. [Online]. Available: https://www.nist.gov/cybersecurity/cybersecurity-awareness-month

[12]

D. P, “Multiple Vulnerabilities in Samsung Products: CERT-In.” Accessed: Jun. 30, 2024. [Online]. Available: https://www.linkedin.com/pulse/multiple-vulnerabilities-samsung-products-cert-in-parthapratim-dash-0pukf

[13]
“Device updates: what’s stopping people from making the change?” Accessed: Jun. 30, 2024. [Online]. Available: https://www.kaspersky.com/blog/device-updates-report/

[14]
DPM, “20 biggest GDPR fines so far [2023],” Data Privacy Manager. Accessed: Jun. 30, 2024. [Online]. Available: https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

[15]
“Google Android version 12.0 : Security vulnerabilities, CVEs.” Accessed: Jun. 30, 2024. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-677097/Google-Android-12.0.html?page=1&order=1&trc=1673&sha=2cea3eeef0b7616e0076f073918175322ea89f64

[16]
W. com / A. Inc, “How Weak Passwords Expose You to Serious Security Risks,” Jetpack. Accessed: Jun. 30, 2024. [Online]. Available: https://jetpack.com/blog/weak-passwords/

[17]
“iPhone vs. Android User & Revenue Statistics (2024),” Backlinko. Accessed: Jun. 30, 2024. [Online]. Available: https://backlinko.com/iphone-vs-android-statistics

[18]
K. W, “Is Android fragmentation still a problem for IT teams? | TechTarget,” Mobile Computing. Accessed: Jun. 30, 2024. [Online]. Available: https://www.techtarget.com/searchmobilecomputing/tip/Is-Android-fragmentation-still-a-problem-for-IT-teams

[19]
K. A, “Vulnerabilities In Samsung Galaxy S22 Expose Devices To Attacks.” Accessed: Jun. 30, 2024. [Online]. Available: https://thecyberexpress.com/vulnerabilities-in-samsung-galaxy-s22-exposed/

[20]
“Knox on Android | Knox features on Android devices,” Samsung Knox. Accessed: Jun. 30, 2024. [Online]. Available: https://www.samsungknox.com/en/knox-platform/knox-on-android

[21]
McAfee, “Remove Malware from Your Android Device,” McAfee. Accessed: Jun. 30, 2024. [Online]. Available: https://www.mcafee.com/learn/how-to-remove-malware-from-android/

[22]
N. K, “Samsung fined $675,000 for a series of privacy violations » The Readable.” Accessed: Jun. 30, 2024. [Online]. Available: https://thereadable.co/samsung-fined-675-000-for-a-series-of-privacy-violations/

[23]
P. T, “Google warns users about 18 vulnerabilities in Samsung Exynos chipsets: Here’s the list of affected devices,” WION. Accessed: Jun. 30, 2024. [Online]. Available: https://www.wionews.com/science/google-warns-users-about-18-vulnerabilities-in-samsung-exynos-chipsets-heres-the-list-of-affected-devices-572942

[24]

"Safety and security updates that take the burden off you," Google. Accessed: Jun. 30, 2024. [Online]. Available: https://blog.google/technology/safety-security/google-cybersecurity-awareness-month-2023/

[25]
"Samsung Galaxy A12 Red," Courts Mammouth | Online Shopping Mauritius. Accessed: Jun. 30, 2024. [Online]. Available: https://www.courtsmammouth.mu/product/samsung-galaxy-a12-red.html

[26]
"Samsung Knox security principles for protection | Samsung Levant," Samsung lb. Accessed: Jun. 30, 2024. [Online]. Available: https://www.samsung.com/lb/sustainability/security-and-privacy/security/

[27]
"Samsung Mobile Security." Accessed: Jun. 30, 2024. [Online]. Available: https://security.samsungmobile.com/workScope.smsb

[28]
"Samsung Products Multiple Vulnerabilities." Accessed: Jun. 30, 2024. [Online]. Available: https://www.hkcert.org/security-bulletin/samsung-products-multiple-vulnerabilities_20240306

[29]
M. Sarwar , "Impact of Smartphone's on Society," *European Journal of Scientific Research 98(2)*, 2013, Accessed: Dec. 31, 2023. [Online]. Available: https://www.researchgate.net/publication/236669025_Impact_of_Smartphone's_on_Society

[30]
R. Satter, "U.S. court: Mass surveillance program exposed by Snowden was illegal," *Reuters*, Sep. 03, 2020. Accessed: Jun. 30, 2024. [Online]. Available: https://www.reuters.com/article/world/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CJ/

[31]
"Millions of Samsung Galaxy owners urged to switch off this Wi-Fi setting immediately - Mirror Online." Accessed: Jun. 30, 2024. [Online]. Available: https://www.mirror.co.uk/tech/samsung-galaxy-bug-exynos-wifi-29485169

[32]
"A malware masquerading as System Update is attacking Android phones," HT Tech. Accessed: Jun. 30, 2024. [Online]. Available: https://tech.hindustantimes.com/tech/news/a-malware-masquerading-as-system-update-is-attacking-android-phones-71616854815372.html

[33]
"Govt issues warning for some Samsung phones, advises urgent update," *The Economic Times*, Dec. 15, 2023. Accessed: Jun. 30, 2024. [Online]. Available: https://economictimes.indiatimes.com/news/new-updates/govt-issues-warning-for-some-samsung-phones-advises-urgent-update/articleshow/106012861.cms?from=mdr

[34]
"Top 7 Mobile Security Threats," www.kaspersky.com. Accessed: Jun. 30, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

[35]
"Verify apps using Play Protect ." Accessed: Jun. 30, 2024. [Online]. Available: https://guidebooks.google.com/online-security/stay-secure-online/verify-apps-play-protect

[36]
“What Are Eavesdropping Attacks?,” Fortinet. Accessed: Jun. 30, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/eavesdropping
[37]
“What is CVE and CVSS | Vulnerability Scoring Explained | Imperva,” Learning Center. Accessed: Jun. 30, 2024. [Online]. Available: https://www.imperva.com/learn/application-security/cve-cvss-vulnerability/
[38]
“What mobile security threats pose a risk to your organisation?” Accessed: Jun. 30, 2024. [Online]. Available: https://www.linkedin.com/pulse/what-mobile-security-threats-pose-risk-your-organisation-tbmye
[39]
“Enter the New Era of Mobile AI With Samsung Galaxy S24 Series.” Accessed: Jun. 30, 2024. [Online]. Available: https://news.samsung.com/global/enter-the-new-era-of-mobile-ai-with-samsung-galaxy-s24-series
[40]
“Stay Secure and Connected with Samsung.” Accessed: Jun. 30, 2024. [Online]. Available: https://news.samsung.com/my/stay-secure-and-connected-with-samsung
[41]
“Apple Platform Security,” Apple Support. Accessed: Jun. 30, 2024. [Online]. Available: https://support.apple.com/guide/security/welcome/web
[42]
“AES-XTS | AES-XTS Storage Encrypt/Decrypt Engine IP Core,” CAST. Accessed: Jun. 30, 2024. [Online]. Available: https://www.cast-inc.com/security/encryption-primitives/aes-xts
[43]
“Google Pixel Privacy & Security Features - Google Safety Center.” Accessed: Jun. 30, 2024. [Online]. Available: https://safety.google/pixel/
[44]
W. C, “What is the Titan M2 security chip in Google’s Pixel phones?,” Android Authority. Accessed: Jun. 30, 2024. [Online]. Available: https://www.androidauthority.com/titan-m2-google-3261547/
[45]
“macOS - Security,” Apple (Latin America). Accessed: Jun. 30, 2024. [Online]. Available: https://www.apple.com/lae/macos/security/
[46]
E. A, “How many Android updates do Samsung, Xiaomi or OnePlus promise?,” nextpit. Accessed: Jun. 30, 2024. [Online]. Available: https://www.nextpit.com/how-many-android-updates-manufactures-offer
[47]
“Security Bulletins for HUAWEI Phones/Tablets.” Accessed: Jun. 30, 2024. [Online]. Available: https://consumer.huawei.com/mu/support/bulletin/#:~:text=The%20monthly%20and%20quarterly%20security,the%20region%20and%20device%20model.
[48]
M. D, “Are iPhones more secure than Android phones? A guide | NordVPN.” Accessed: Jun. 30, 2024. [Online]. Available: https://nordvpn.com/blog/ios-vs-android-security/
[49]

"Customization Service - SAMSUNG," Samsung Electronics America. Accessed: Jun. 30, 2024. [Online]. Available: https://www.samsung.com/us/account/customization-service/

[50]
"Make your iPhone your own," Apple Support. Accessed: Jun. 30, 2024. [Online]. Available: https://support.apple.com/guide/iphone/make-your-iphone-your-own-iphefb3daa42/ios

[51]
"Events," Cybersecurity Collaboration Forum. Accessed: Jun. 30, 2024. [Online]. Available: https://www.cybersecuritycollaboration.com/events

[52]
"Samsung Knox Documentation." Accessed: Jun. 30, 2024. [Online]. Available: https://docs.samsungknox.com/admin/

[53]
"Are iPhones more secure than Android devices? | TechTarget," Mobile Computing. Accessed: Jun. 30, 2024. [Online]. Available: https://www.techtarget.com/searchmobilecomputing/tip/Are-iPhones-more-secure-than-Android-devices

[54]
SamMobile and A. Mishra, "When will my Galaxy phone get a security update?," SamMobile. Accessed: Jun. 30, 2024. [Online]. Available: https://www.sammobile.com/samsung/samsung-galaxy-security-updates

[55]
C. L, "User Interface Matters: Analysing the Complexity of Mobile Applications from a Visual Perspective," 2021, Accessed: Jun. 30, 2024. [Online]. Available: https://www.sciencedirect.com/

[56]
"Manage Application Permissions for Privacy and Security | CISA." Accessed: Jun. 30, 2024. [Online]. Available: https://www.cisa.gov/resources-tools/training/manage-application-permissions-privacy-and-security

[57]
"OWASP Mobile Top 10 | OWASP Foundation." Accessed: Jun. 30, 2024. [Online]. Available: https://owasp.org/www-project-mobile-top-10/