STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jsrm.thestap.com/

Check for updates

Analyzing Cybersecurity Threats on Mobile Phones

Sara Alsahaim[1], Mohammed Maayah[2]

[1] *College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia*
[2] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*

ARTICLE INFO

Article History

Received: 17-03-2023
Revised: 30-05-2023
Accepted: 11-08-2023
Published: 12-08-2023

Vol.2025, No.3

DOI:
https://doi.org/10.63180/jsrm.thestap.2023.1.2

***Corresponding author.**
Email:
mohammad7ups@yahoo.com

Orcid:
https://orcid.org/0009-0008-9785-485X

ABSTRACT

The widespread digital transformation has deeply integrated mobile devices into the fabric of daily life, making them indispensable tools for communication, education, healthcare, and financial transactions. However, the increasing reliance on mobile technology has also introduced a growing landscape of security threats and vulnerabilities. This research aims to systematically analyze the security risks associated with mobile phone usage, identify their underlying vulnerabilities, and propose effective countermeasures. With many users lacking adequate awareness of cybersecurity practices, mobile devices become susceptible to threats such as malware, phishing, unauthorized data access, and malicious applications. The study focuses on both individual and organizational perspectives, emphasizing that threats at the personal level can propagate to broader domains such as workplaces and educational environments. Utilizing a systematic literature review guided by the PRISMA methodology, relevant studies published between 2016 and 2022 were examined through databases like the Saudi Digital Library and Google Scholar. The research addresses three central questions: (1) what are the prevalent security threats on mobile phones? (2) What vulnerabilities contribute to these threats? (3) What countermeasures are most effective in mitigating them? The findings highlight the urgent need for user education and implementation of security tools, such as antivirus applications and safe downloading practices, to fortify mobile security and reduce potential risks.

Keywords: Cybersecurity; Threats; Mobile Phones; Vulnerabilities; Mobile Security.

How to cite the article
Alsahaim, S., & Maayah, M. (2023). Analyzing Cybersecurity Threats on Mobile Phones. STAP Journal of Security Risk Management, 2023(1), 3–19. https://doi.org/10.63180/jsrm.thestap.2023.1.2

1. Introduction

There has been a digital transformation in all fields from traditional paper form to the digital form. Thus, technology has entered the user's life at all levels in his life. At the first, computers appeared and become an essential thing in the daily routine until mobile devices developed and become the current modern small shape that enables the user to di all his needs through his device, such as booking appointments in hospitals, following up on educational lessons, and paying his monthly bills. Mobile devices become now a basic thing in the people lives to perform their daily works and routine [1].

With this great and rapid development that has occurred in the place of the mobile devices in our daily lives, on the other side there is a rapid development in the threats such as malware that may affect mobile devices especially while the last years because the increase of the use of mobile devices, attackers always try to find vulnerabilities through they could attack and penetrate mobile devices [2].

Unfortunately, many people do not have enough knowledge of the ways to protect their devices and protect their personal data With this technical development and the development in the use of mobile devices also the development in the technical risks and threats the devices may face, there is an urgent need to take appropriate countermeasures to protect the devices and the user of the device from any threats in also to reduce the possible risks. Mobile phones are now used at every moment and in all fields. Threats on mobile phones have been evolved with this tremendous progress and researchers are now interested in analyzing and identifying risks, identify the vulnerabilities that may cause them to occur that may face their user in order, to define a set of potential risks and their countermeasures, as when these countermeasures implemented, the risks are reduced [3].

Risk analysis in mobile phones at the individual user level, it protects his data and transaction and all his technical resources from any expose or risks, also the protection of the individual extends to protect the scope in which he is, whether a company, institution, work, or educational domain [4]. The risks in using mobile phones are interrelated, thus when an individual is affected, the danger may extend to those around him. The aim of this research is to identify the threats in mobile phones and their countermeasures to reduce them. Mobile phones at this time with its modernity and the technology development have become an essential thing in people lives. With this technology development, security threats in mobile phones have evolved band have various types. Therefore, analyzing the vulnerabilities and the appropriate countermeasures to confront these is a very important issue [5].

Mobile phones are a fertile environment for risks, as the user depends on them in his daily routine of communicating, sharing files and browsing. This use of the mobile phones may contain some risks for example, when the user is downloading an application from untrusted source this application could be a malicious application, one of the countermeasures for malicious applications is downloading the applications is install apps from trusted source [3], another example files that are shared may contain malwares cause harm to the device and the user such as spying. This harm that threats might cause could affect in the user in a badly way, the suggested countermeasure is installed mobile security and antivirus application [2]. While these risks could be reduced when appropriate security countermeasures are taken also with the user awareness. The analysis of security threats on mobile phones contains two main domains must be focused to reduce risks, which are user domain and workstation domain. The expected outcomes of this research are reviewing a collection of articles related of the security risks on mobile phones and based on these articles we will get answer on the following questions:

1. What are the possible security threats on mobile phones?
2. What are the vulnerabilities that cause threats on mobile phones?
3. What are the suggested countermeasures to mitigate the threats?

2. Research Methodology

In order to this systemic review, four steps have been carried in PRISMA, in the first stage these research strings have been formulated as:

Threats (vulnerabilities OR risks OR challenges) on Mobile (cell) AND Phones (devices). The search contacted in the

Saudi digital library and google scholar database with the following inclusion criteria: papers are represented threats on mobile phones between the years 2016, and 2022.

Where the exclusion criteria were as the following: Papers are not related to the topic, Duplication, papers that not accessible. In the first stage: the identification stage 163000 was founded in the different database, after removing the duplication 400 papers are remined, 250 papers have been excluded which not matching the criteria. after a full text assessing, in the included phase, 50 studied chosen, 15 of them were excluded to end up with 35 selected studies, this shown in the Figure 1.

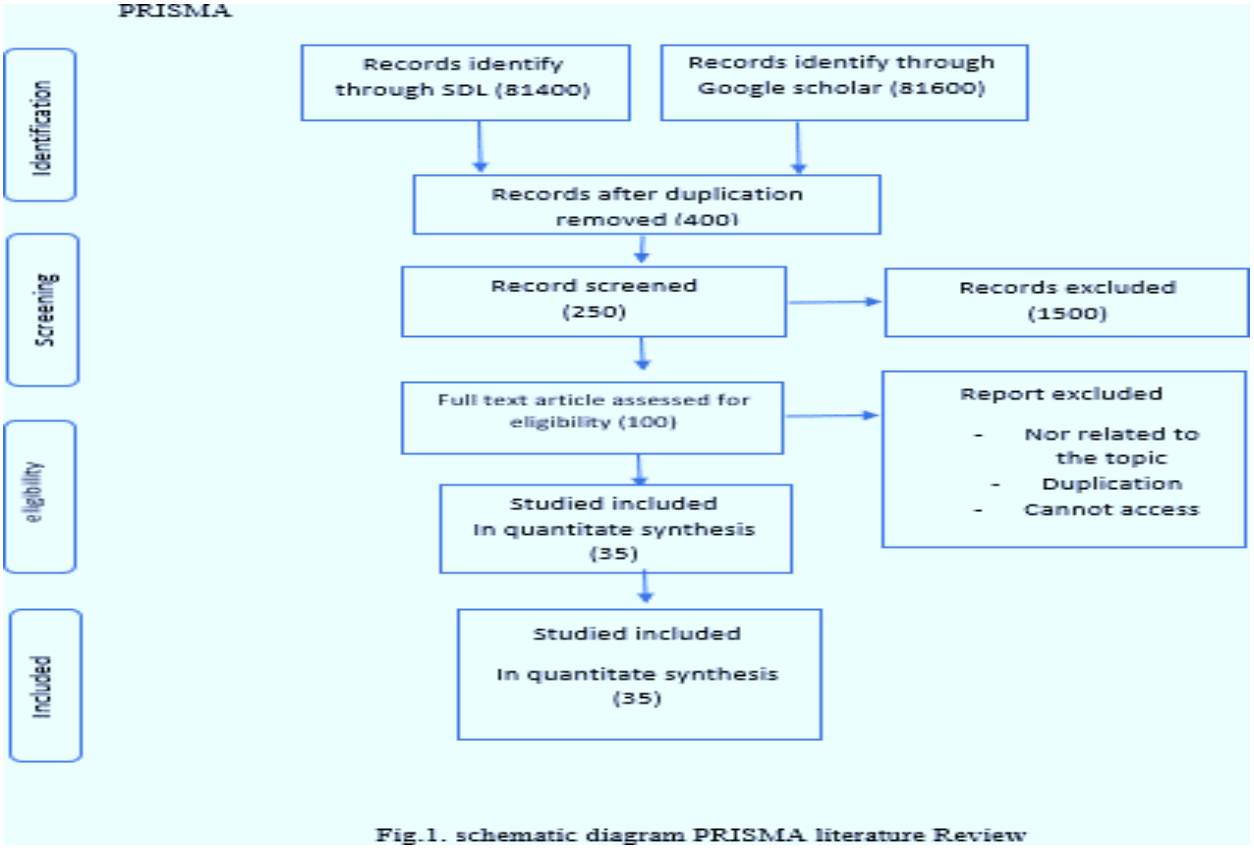

Figure 1. Research methodology.

3. Existing Works

In this research several studies have been reviewed which related to threats on mobile phones, the studies are between the years 2016 and 2022, the studies will be analyzed and the following will be illustrated the objective of each article, problem statement of each article, type of the article, the methodology used in each article, findings of each article and contribution of each article. In the study of Murat Yesilyurt and Yildiray Yalman [1], the authors performed a review on Security threats on mobile Devices and their Effects: Estimations for future, the study have discussed the four mobile operating systems which they are (Android, Apple OS (iOS), Symbian and Java ME), the objective of this study is to know what is the most common operating system that sending malware through, also the researchers address the threats of mobile operating systems vulnerabilities, malware and attacks, the study shows that is the Android operating system is the most OS which is sending malware through, also they show that is Apple IOS is the most secure operating system because of its closed code, as the authors used qualitative and quantitative approaches in their study. In the study of Pawel Weichbroth and Lukasz Lysik [2], the authors reviewed an article on Mobile security: threats and best practices, the researchers address mobile security threats such as malware, Phishing, data leakage, direct hacker attacks, stolen and lost mobile phones, and social engineering, and the study contribute by illustrating the best practices for having a good security foe the mobile devices, as the authors used a qualitative approach in their study.

In the study of Milad Taleby Ahvanooey, Prof.Qianmu Li,Mahdi Rabbani and Ahmed Raza Rajput [3],The authors performed a survey on smartphones security: software Vulnerabilities, Malware, and attacks, the authors aim of their study was to survey the operating systems and their security features also the possible threats and vulnerabilities, as well as the study identify the security solutions for users and researchers, as the authorsused qualitative and quantitative approaches in their study. In this study of Yasmin Salah Ibrahim Hamed, Sara Nabil Abdullah Abdulkader, and Mostafa Sami M. Mostafa [4], the authors performed a survey on Mobile Malware Detection, the study illustrated the different type of malware and their operating systems platform, the study also illustrated the typed of mobile malware detection methods and the mobile detection typed which they are host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS) ,as the authors used a qualitative approach in their study. In this study of Teodor Mitrea, Monica Borda [5], the authors performed a survey on Mobile Security Threats: A Survey on Protection and Mitigating strategies, the study discuss the vulnerabilities that face the technical environment of the mobile devices such as the poor encryption and the inefficient TLS protection, as the authors used a qualitative approach in their study. In the study of Ioan Adascalitel [6], the author performed a review on smart phones and IOT security, the study illustrated the increasing of using smart phones and the different potential threats, the study analyzed threats into two categories the first physical threats and vulnerabilities such as lost device or damage device, the second one software-based threats and vulnerabilities such as threats on the network level when the device is connected to unsecure network, as the authors used a qualitative approach in their study.

In the study of Drajad Wiryawan, Joni Suhartono, Surjandy, Yudi Fernando, Idris Gautama so, and Anderes Gui [7], the authors performed a review on malware mobile devices in Indonesia, the study method is qualitative approach and the study identify the basic user behavior on mobile malware for user profile analysis, as the study analyze user behavior in three categories maintenance, operation and modification and thy found that the users must perform maintenance to protect against most threats, as the authors used a qualitative approach in their study. In this study of Aakash Ahmad, Asad Waqar Malik, Abdulrahman Alreshidi, Wilayat Khan, and Maryam Sajjad [8], the authors performed a review on Adaptive Security for Self-Protection of Mobile Computing Devices, the study illustrated the mobile computing and its challenges, as the study purposed a frame work which protect the critical resources of mobile devices (hardware sources, software sources), the frame work monitor the hardware and software resources at the running time and detect if there any unauthorized access, as the authors used a qualitative approach in their study. In the study of A B M Kamrul Riad, Md Saiful Islam, Hossain Shahriar, Chi Zhang, Maria Valero, Sweta Sneha, and Sheikh Ahamed [9], the researchers performed a review on Plugin-based Tool for Teaching Secure Mobile Application Development, the researchers address mobile application threats , the study suggested a DroidPlatrol plugin for Android operating systems as they illustrated a DroidPlatrol plugin helps in identifying the vulnerabilities in application security, as the authors used a qualitative approach in their study.

In the study of Douglas Kunda and Mumbi Chishimba [10], the researchers performed a survey on A Survey of Android Mobile Phone Authentication Schemes, the study illustrated the mobile security threats such as shoulder surfing, guessing and duplicates, Malware, broken cryptography and social engineering and the role of authentication to protect the mobile device against unauthorized access, as the researchers used a qualitative approach in their study. In this study of Ashwag Albakri, Huda Fatima, Maram Mohammed, Aisha Ahmed, Aisha Al, Asala Ali, and Nahla Mohammed Elzein [11], the researchers performed a Survey on Reverse- Engineering Tools for Android Mobile Devices, the study aims to illustrate the Android operating system architecture, as they defined, as the researchers used a qualitative approach in their study. In the study of Mansour Alsaleh1, Noura Alomar, and, Abdulrahman Alarifi [12], the researchers reviewed an article on Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods, their study addresses the security risks in mobile phones and they analyze them based on the user practices as the following using public network, accept the accessing on their location services, as the researchers used a qualitative approach in their study. In the study of Esmeralda Kadëna [13], the researcher reviewed an article on smartphones security threats, the researcher illustrated the different types of attacks and they analyzed into categories (hardware based, software based, user based, phishing attacks, SSL proxy attacks, camera-based vulnerabilities attack, as the researchers used a qualitative approach in their study. In the study of Maryam bubkair and mohammed almaiah[14], the researcher performed a scurvy on cybersecurity concerns on smartphones and application , the researcher illustrated the different types of such as poor authentication mechanism, unsecure Wi-Fi ,confidential data leakage, malicious code injection, , as they identify the possible attacks such as denial of service, as the researchers used a qualitative approach in their study.

In the study of Alin Zamfiroiu et al. [15], the researcher reviewed an article on mobile data vulnerabilities, the researchers illustrated the hardware threats such as cold boot attack and the software threats such as malware attack, as the researchers used a qualitative approach in their study. In the study of Shima Alhashim et al. [16], the researchers reviewed literature review on cybersecurity threats in line with awareness in Saudi Arabia, their study addresses the mobile security threats in Saudi Arabia and the awareness rate between the individual, as the researchers used a qualitative and quantitative approach in their study. In the study of S. T. Amanzholova et al. [17], the researchers a review on analysis of threats for mobile devices and methods of protection, their study addresses the mobile security threats malicious software, social engineering attacks, attacks through web applications and network, data leakage, as the researchers used a qualitative approach in their study. In this study of Hamid Reza Nikkhah et al. [18], the authors performed a review on mobile application security role of privacy, the study illustrated the privacy concerns in the mobile phones' applications and one of the concerns is the improper access by a third party, as the researchers used a qualitative approach in their study. In this study of Mohammed AlJutail et al. [19], the authors performed a survey on associated risks in mobile applications permissions, the study illustrated the role of the applications permissions on the user security, as the permission could be harmful to the user such as switching on the camera for spying, the authors in the study shows that users don't spend time to understand the type of required permission for the applications, so user awareness is a need , as the researchers used a qualitative approach in their study.

In this study of Gouoyon Koala et al. [20], the authors performed a review on analysis of the impact permissions on the vulnerability of mobile applications, the study analysis the risks of the permission and the ability to use them to access sensitive data, as the researchers used a comparison approach in their study. In this study of Syed Farhan Alam Zaidi et al. [21], the authors performed a survey on A Survey on Security for Smartphone Device, the study illustrated the Structure of Smartphones Operating System and the vulnerabilities such as System Fault / Defects, Insufficient Management of Apps, Unsecure Wireless Network, Lack of User Awareness as the researchers used a qualitative approach in their study. In this study of Mine Zeybek et al. [22], the authors performed a review on security awareness in mobile devices, the study illustrated the threats in mobile devices such as the ability of some applications to run and download other applications without the user knowledge, as the researchers used a qualitative approach in their study. In this study of Maniah et al. [23],the authors performed a survey in threats and risks in cloud computing environment, the authors address the threats in cloud computing and classify the threats into four groups and under each group there are several of threats, threats to applications threats to data, threats to infrastructure, threats to cloud services in general such as sniffing and spoofing, as the researchers used a qualitative approach in their study. In this study of Tauseef Ibne Mamun et al. [24] the authors performed A Survey on Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcoming Those Vulnerabilities, the study illustrated the android threats such as spam, malware, data hijacking, permission, rooting, as the researchers used a qualitative approach in their study. In this study of Didier Bassole et al. [25] the authors performed A review on vulnerabilities analysis in mobile banking and payment applications on android in Africa countries, the study illustrated the android threats such insecure data storge, insecure transmission of data, as the researchers used a qualitative approach in their study. In this study of Martin butler et al. [26], the authors performed A review on the influence of mobile operating systems on user security behavior, the study threats detection based on behavioral studies focusing on different aspects of smartphone user behavior, because the user behavior is affecting on the security aspects in his device, as the researchers used a qualitative approach in their study.

In this study of Asma K [27], the author performed A review on Android permission system and user privacy a review of concepts and approaches, the study illustrated the dangerous permissions for the android operating system and their effect on the user privacy, as the author used a qualitative approach in their study. In this study of Erza Gashi et al. [28], the authors performed A review on permission- based privacy analysis for android applications , the study illustrated the dangerous of application permissions for the android operating system and how they could be a vulnerability through them spy on the user such as the microphone and camera permissions ,also the study shows there is no specific stated to classify the permission is safe or not as the researchers used a qualitative approach in their study. In this study of Sunali Jogsan et al. [29], the authors performed A survey on permission- based malware detection in android applications, the study illustrated the detect of android malware applications based on permissions, as the researchers used a qualitative approach in their study. In this study of Dr sonali M Kothari et al. [30], the authors performed A review on static analysis of android permissions and SMS using Machine learning algorithm, the study illustrated the detect of android malware applications based on permissions, as the researchers used a qualitative approach in their study. In this study of Rika Butler [31], the authors performed a systemic literature review of the factors affecting smart phones user threats avoidance behavior, the study illustrated six factors affecting in the security on the smartphones and they are 1. Knowledge and awareness. 2. Misconceptions and trust.3. Cost and benefit considerations.4. Carelessness. 5. Received measure effectiveness.6. The

user's perceived skills and efficacy, as the researchers used a qualitative approach in their study. In this study of Nikhat Akhtar et al. [33], the authors performed a comprehensive overview of privacy and data security for cloud storge, the study illustrated the cloud data storge and the threats and privacy threats in cloud data storage the study analyze such as data breaches and denial of service which effect on the availability, as the researchers used a qualitative approach in their study. In this study of Nashwan saeed M Ghaleb Al-Thobhant et al. [34], the authors performed a review on cloud computing security solutions and privacy, the study illustrated the security challenges on the cloud computing such as vulnerabilities on the cloud because of the outsourced computing. Thus, cloud systems could face different attacks which effect on the mobile devices and breach them, as the researchers used a qualitative approach in their study. In this study Abrar Atif Asghar [35], the author review am article on Major security challenges of cloud computing technology, the study illustrated the challenges on cloud computing such as data security and software security as the researcher used a qualitative approach in their study.

Table 1. Related Works.

Authors	Name of the article	Publication year	Address threats	Suggested mitigation
Murat Yesilyurt et al. [1]	Security threats on mobile Devices and their Effects: Estimations for future	2016	- Malware: Torjans - Virus - Spyware: adware, cookies - Rooting (jailbreaking)	- Downloading applications is limited to downloading them from the official operating system store.
Pawel Weichbroth et al. [2]	Review Article Mobile security: threats and best practices	2020	- Malware: Android GMBot-spyware - Acedeviver IOS malware - Social engineering and Phishing	- The operating system should keep up to date. - Running antimalware app - Do not response to tricky messages - Keeping applications up to date - Enable remote data wipe - Disable Bluetooth and Wi-Fi when not needed - Do not able unnecessary permissions to applications - Install mobile security and antivirus application
Milad Taleby Ahvanooey et al. [3]	A survey on smartphones security: software Vulnerabilities, Malware, and attacks	2017	- Malicious applications (malware, virus, spyware, torjan, rootkit) - Social engineering - Phishing apps	- Install apps from trusted sources - Install mobile security software - Prevent root, Jailbreaking - The security of the network - Keep smartphone OS up to date

Yasmin Salah Ibrahim Hamed et al. [4]	Mobile malware detection : A survey	2019	- Network based malware (adware, cookies, spam, mobile spyware) Ordinary based malware (virus, worm)	- Mobile malware detection algorithms: - Classification algorithm - Static techniques (the analysis of detection source code) Signature based analysis Permission based analysis Virtual machine analysis - Dynamic techniques Emulation based analysis Anomaly based analysis Taint analysis
Teodor Mitrea et al. [5]	Mobile Security Threats: A Survey on Protection and Mitigating strategies	2020	- Unauthorized access to the sensitive data - Insufficien t TLS protection - Data leakage	- Encryption - Authentication - Multi factor authentication for application has high degree of sensitivity - Restrict data collection - Managing cookies
Ioan Adascalitel [6]	smart phones and IOT security	2019	- Physical threats (stolen, damaged, and lost devices) - Software-based threats (network level man in the middle, phishing) -	- Connect to a trusted network - Encryption - Educate the user
Drajad Wiryawan et al. [7]	Malware mobile devices in Indonesia	2019	- User behavior	- perform maintenance
Aakash Ahmad et al. [8]	Adaptive Security for Self-Protection of Mobile Computing Devices	2019	- Unauthorized access	-Monitoring framework
A B M Kamrul Riad et al. [9]	Plugin-based Tool for Teaching Secure Mobile Application Developme nt	2021	- application threats (rooting, jailbreaking)	DroidPlatrol plugin for Android operating system

Douglas Kunda et al. [10]	A Survey of Android Mobile Phone Authentication Schemes	2018	-	unauthorized access	- pass word/pin code authentication - pattern authentication - biometric authentication - facial recognition	
Ashwag Albakri et al. [11]	Survey on Reverse-Engineering Tools for Android Mobile Devices	2022	-	Insecure Data Storage - SQL/HQL Injection	- APKInspector - AndroBugs Framework	
Mansour Alsaleh1 et al. [12]	Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods	2017	-	User practices - Connecting to public network - Sharing location	- Do not connecting to public net work - Limit the accesses to location services	
Esmeralda Kadëna[13]	article on smartphones security threats	2017	-	Malware - Attacks based on software, hardware, user - Phishing attacks - SSL proxy attacks	- Strong password authentication - Do not rooting - Be aware of phishing	
Maryam bubkair et al. [14]	cybersecurity concerns on smartphones and application	2021		- poor authentication mechanism, unsecure Wi-Fi, confidential data leakage, malicious code injection, , as they identify the possible attacks such as denial of service	- Update apps and operating system - Install mobile security software - Educate the user - Finding monitoring mechanisms operating network to detect malicious attacks - Multi factor authentication	
Alin Zamfiroiu et al. [15]	mobile data vulnerabilities	2019		- hardware threats such as cold boot attack and the software threats such as malware attack	- updating OS - encryption - Password	

Shima Alhashim et al. [16]	cybersecurity threats in line with awareness in Saudi Arabia	2021	- Malware - Account hijacking	- Awareness
S. T. Amanzholova et al. [17]	analysis of threats for mobile devices and methods of protection	2019	- malicious software, social engineering attacks, attacks through web applications and network, data leakage	- use personal firewall - monitor and unavailability of password for another person - install security application against the malicious software
Hamid Reza Nikkhah et al. [18]	mobile application security role of privacy	2018	- improper access	- develop applications with strict privacy
Mohammed AlJutail et al. [19]	associated risks in mobile applications permissions	2019	- harmful access to the mobile resources	- awareness - automated application - install application from trusted source - revoke sensitive permission rem applications
Gouoyon Koala et al. [20]	analysis of the impact permissions on the vulnerability of mobile applications	2020	- risks of harmful permissions	- improve user od - have only one signature per app - appropriate mechanisms to approve third-party libraries used in app development
Syed Farhan Alam Zaidi et al. [21]	A Survey on Security for Smartphone Device	2016	- Physical Attack - Virus - Relay Attack	- Re-manufacturing whether is software or hardware - Install update Antivirus in your system. - Use secure network and trusted proxy application.
Mine Zeybek et al. [22]	security awareness in mobile devices	2019	- the ability of some applications to run and download other applications without the user knowledge	- raise the user awareness in the permissions
Maniah et al. [23]	survey in threats and risks in cloud computing environmet	2020	- threats to applications - threats to data - threats to infrastructure - threats to cloud services in general such as sniffing and spoofing	

Tauseef Ibne Mamun et al. [24]	Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcomig Those Vulnerabilitis	2016	-	spam, malware, data hijacking, permission - rooting - install time granting access without reading the permission list		
Didier bassole et al. [25]	vulnerabilities analysis in mobile banking and payment applications on android in Africa countries	2020	-	insecure data storage, insecure transmission of data	-	restrict application permission - secure transmission of sensitive data - using existing cryptography -
Martin butler et al. [26]	the influence of mobile operating systems on user security behavior	2021	-	Threats in the operating system	-	behavioral studies focusing on different aspects of smartphone user behavior
Asma K [27]	Android permission system and user privacy a review of concepts and approaches	2017	-	application permissions	-	permission managing - user awareness
Erza Gashi et al. [28]	permission-based privacy analysis for android applications	2017		- android application permissions		

Sunali Jogsan et al. [29]	A survey on permission-based malware detection in android applications	2020	-	Malware applications	-	Secure Sockets Layer (SSL) - CleanOS(encrypt sensitive data snd save keys in the cloud) - TinMan(sapertate confidential data) - Sentry (secure the keys, prevent store them in the RAM)
Dr sonali M Kothari et al. [30]	static analysis of android permissions and SMS using Machine learning algorithm	2018	-	Bootnet attack	-	static analysis of SMS and Android permissions and is designed for network service providers. In dynamic analysis, prevention method for user device is provided.
Rika Butler [31]	A systemic literature review of the factors affecting smart phones user threats avoidance behavior	2020	-	risky behavior such as jailbreaking phones and then loading unverified apps on phones - connected to unsecure network	-	addressing human behavior is crucial in the fight against mobile threats and reduce it by educate the user
Rahul Neware et al. [32]	survey on security issues in mobile clouding computing and preventive measures	2020	-	Data security issues (data loss for the data stored in the clouds) - Mobile cloud application challenges (malware, worm)	-	Public and private keys - Encryption - Digital signature
Nikhat Akhtar et al. [33]	a comprehens ive overview of privacy and data security for cloud storge	2021	-	Denial of service - Data breaches	-	Update operating system - Encryption mechanism - Access control
Nashwan saeed M Ghaleb Al-Thobhant etal.[34]	cloud computing security solutions and privacy	2021	-	Different attacks on the cloud system	-	robust security scheme and user- centric security policy is implemented

Abrar Atif Asghar [35]	Major security challenges of cloud computing technology	2020	- challenges such as: - data security - software security - Encryption

4. Analysis

In this research the reviewing was on thirty-five papers, the papers were selected based on the relation to the research title also the publication year between 2016 and 2022, the following Fig2 illustrated the percentage for publication year for the scientific paper and the number of papers analyzed in this research. As three papers in 2016 were analyzed in this research, while five papers were in 2017, and three papers also were in 2018, while eight papers were in 2019, also nine papers were in 2020, six papers in 2021, and a paper in 2022.

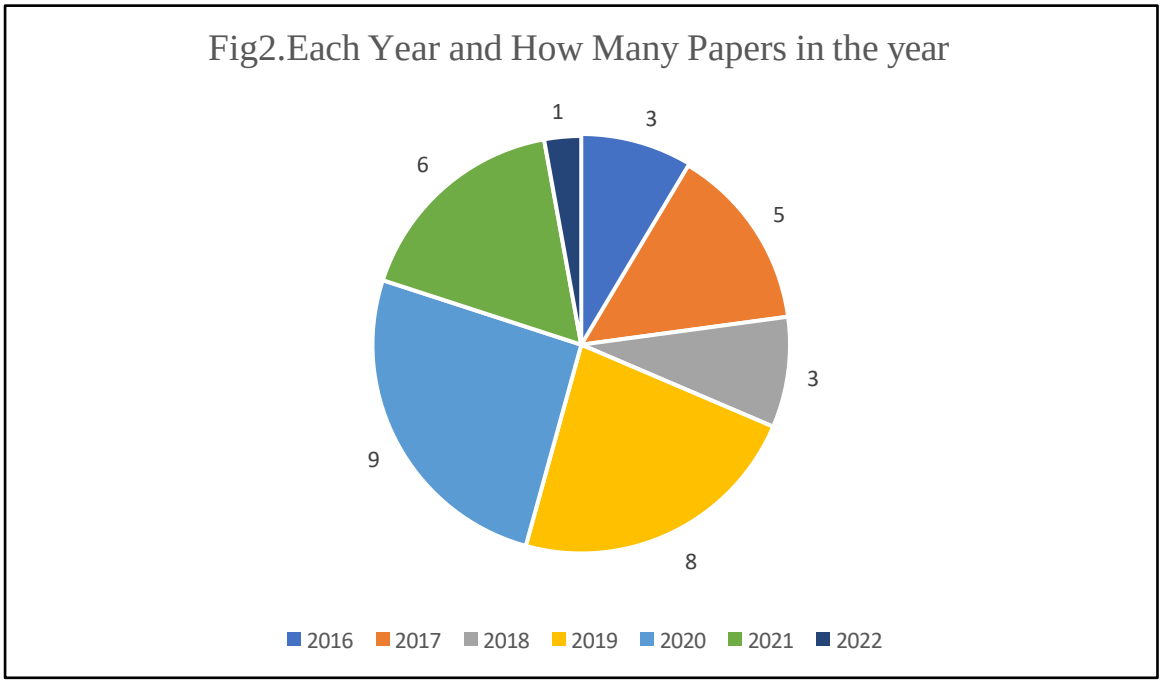

Figure 2. Distribution of research by year.

4.1 Identify the Common threats on the mobile phones

Mobile phones threats are varied, and with the development of the technology, many types have appeared, but there are still some types are more common than others based on the previous scientific papers as shown in the Figure 3, thus in this section will explain each of the common threats:

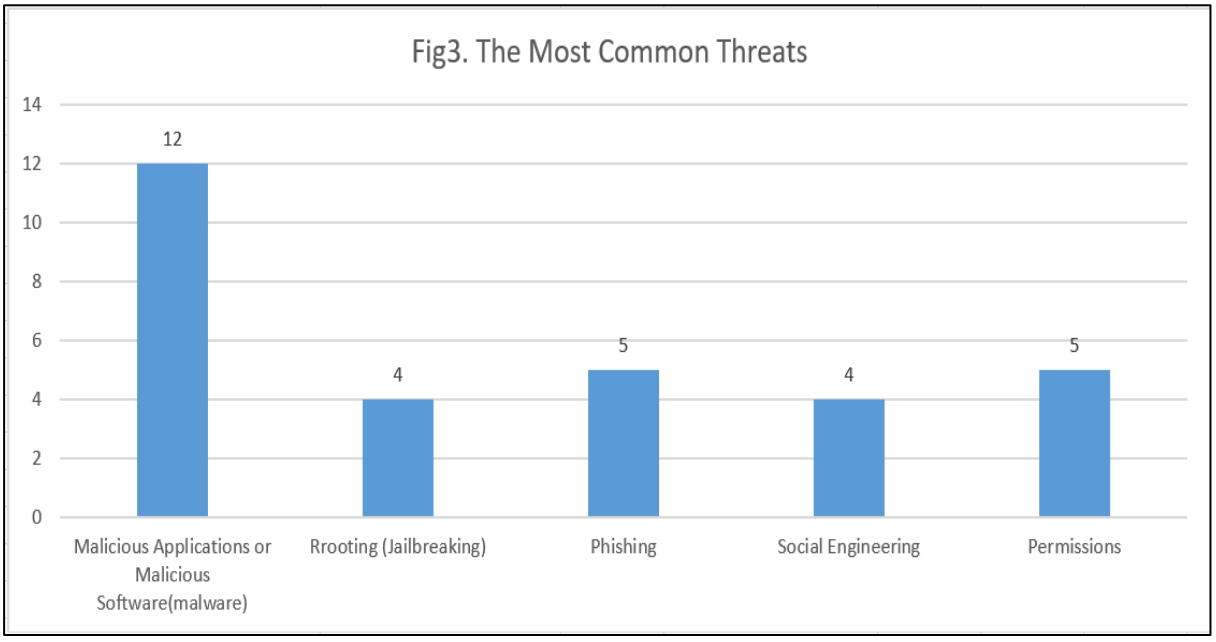

Figure 3. Findings of the most common threats.

4.1.1 Malicious Software (malware) or malicious applications:

Malicious software is aimed at private specific information which disturb users, may cause breakdown of the device and lead to result such as causing information and document belonging to the user to be stolen or become unusable. Such as Torjan, Adware, worm, virus. [1]. "Malicious applications is a hidden malware that can operate in the background of the victim's smartphone." [3], also the malicious applications can be active without knowing of the mobile user or the anti-malware.

4.1.2 Rooting (Jailbreaking):

"Root exploit for mobile phones are coveted by two different two of people: malware authors and smart phone user who want to modify their phones. Malware authors can use root exploit to gain extra privileges and perform any operations on the phone, for example attacker can use a root exploit on an android phone to gain access to the API thar are supposed to be protected by the permission system" [36].

4.1.3 Phishing:

Phishing is such as fraud emails targeting the user in order to obtain his credentials. Not just emails also sometimes becomes phishing apps" is one of the malware which is designed exactly same the real app for stealing sensitive information such as username and passwords." [3]

4.1.4 Social Engineering:

The simplest definition of the social engineer is relying in the user's lack of awareness to disclose his personal information and then exploiting them to attack him. For example, one of the most social engineering frauds is a person calling claiming to be an employee of your bank and asking for your information to update, which is actually a fraud to steal the user bank account.

4.1.5 Permissions:

All the applications in the mobile phones have set permissions, the user can accept or reject them, where some of these permissions are not needed by the application, such as permission to access to the device's camera for an application the purpose of it order food, thus giving the application permission to access a source of the device that it does not need it, is a major threat on the user privacy.

4.2 Identify Vulnerabilities

Vulnerabilities are the likelihood in the system that enables the attacker to exploit the system and perform the attack, such as the lack of the awareness is a vulnerability in a part of the system which is the user, by performing the social engineer or any available vulnerability.

4.3 Identify the Suggested Countermeasures

In this section the discussion will be about the countermeasure to avoid the possible threats and reduce them. As we previously reviewed the most common threats on the mobile phones, now the review will be for the suggested countermeasures that were mentioned in the scientific papers to mitigate these threats, they are: downloading the applications from trusted source, install mobile security and antivirus application, keep the operating system and the application up to date, awareness, and permission managing, as shown in the following Figure 4. The following Table 2 illustrated threats and their countermeasures:

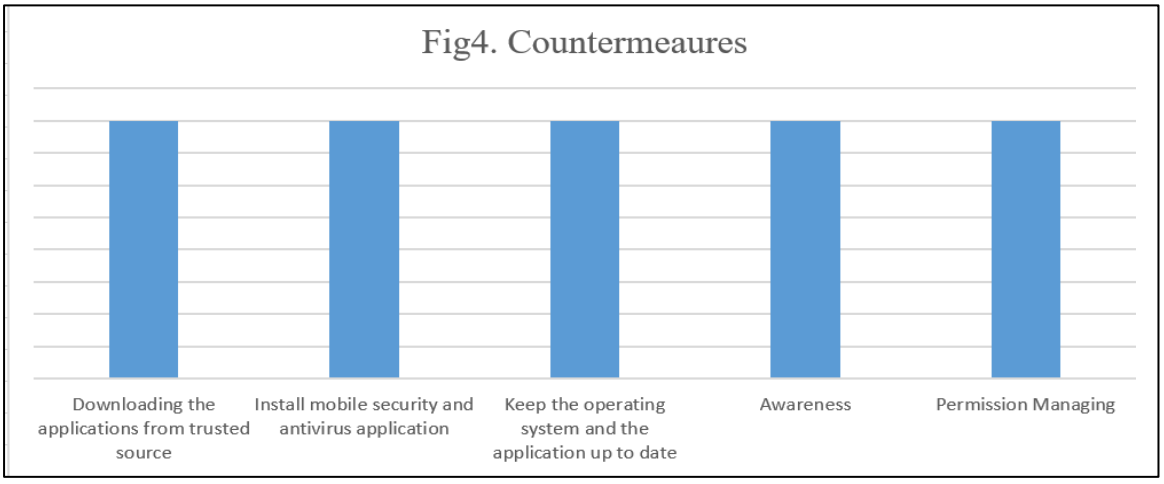

Figure 4. Findings of the main countermeasures.

Table 2. illustrated threats and their countermeasures

Threat	Countermeasure
Malicious Software(malware) or Malicious applications	- Install security application. - Keep the operating system and the application up to date. - Downloading the applications from trusted source.
Rooting (Jailbreaking).	- Prevent Rooting (Jailbreaking).

Phishing.	- User awareness of phishing. - Do not response to tricky messages.
Social engineer.	- Awareness. - Do not response to tricky messages.
Permissions.	- Permission managing. - User awareness. - Revoke sensitive permission rem applications

5. Conclusion

In this research, the aim was to review and analyze papers related to threats on mobile phones to define what are threats facing the mobile phones in the current time and what are the countermeasures to reduce them. After analyzing the scientific papers, it becomes clear that there is a key factor to confront threats, which is user awareness, many of the countermeasures that must be done to reduce mobile phone threats must be done by the user, such as updating the operating system, download applications from trusted source, nor responding to fraud from fake links or calls. Threats on mobile phones become a main issue to study and analyze to find the best solutions to protect devices and information in order to protect the user.

Corresponding author

Mohammed Maayah
mohammad7ups@yahoo.com

Acknowledgements
Not applicable.

Funding
No funding.

Contributions
S.A; M.M; Conceptualization, S.A; M.M; Investigation, S.A; M.M; Writing (Original Draft), S.A; M.M; Writing (Review and Editing) Supervision, S.A; M.M; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] Yesilyurt, M., & Yalman, Y. (2016). Security threats on mobile devices and their effects: estimations for the future. International Journal of Security and Its Applications, 10(2), 13-26.

[2] Bissyandé, T. F., & Sié, O. (2020, February). Analysis of the Impact of Permissions on the Vulnerability of Mobile Applications. In e-Infrastructure and e-Services for Developing Countries: 11th EAI International Conference, AFRICOMM 2019, Porto-Novo, Benin, December 3–4, 2019, Proceedings (Vol. 311, p. 3). Springer Nature.
[3] Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone device. International journal of advanced computer science and applications, 7(4), 206-219.
[4] Hamed, Y. S. I., AbdulKader, S. N. A., & Mostafa, M. S. M. (2019). Mobile malware detection: A survey. International Journal of Computer Science and Information Security (IJCSIS), 17(1).
[5] Mitrea, T., & Borda, M. (2020, June). Mobile security threats: a survey on protection and mitigation strategies. In International Conference Knowledge-Based Organization (Vol. 26, No. 3, pp. 131-135).
[6] Adăscăliței, I. (2019). Smartphones and IoT Security. Informatica Economica, 23(2).
[7] Wiryawan, D., Suhartono, J., Fernando, Y., So, I. G., & Gui, A. (2019). Malware Mobile Devices in Indonesia. KnE Social Sciences, 259-267.
[8] Ahmad, A., Malik, A. W., Alreshidi, A., Khan, W., & Sajjad, M. (2019). Adaptive security for self-protection of mobile computing devices. Mobile Networks and Applications, 1-20.
[9] Riad, A. B. M., Islam, M. S., Shahriar, H., Zhang, C., Valero, M., Sneha, S., & Ahamed, S. (2021). Plugin-Based Tool for Teaching Secure Mobile Application Development. Information Systems Education Journal, 19(2), 25-34.
[10] Kunda, D., & Chishimba, M. (2018). A survey of android mobile phone authentication schemes. Mobile Networks and Applications, 1-9.
[11] Albakri, A., Fatima, H., Mohammed, M., Ahmed, A., Ali, A., Ali, A., & Elzein, N. M. (2022). Survey on Reverse-Engineering Tools for Android Mobile Devices. Mathematical Problems in Engineering, 2022.
[12] Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. PloS one, 12(3), e0173284.
[13] Kadëna, E. (2017). Smartphone Security Threats. Manag. Enterp. Benchmarking 21st century, 141- 160.
[14] Bubukayr, M. A. S., & Almaiah, M. A. (2021, July). Cybersecurity concerns in smart-phones and applications: A survey. In 2021 International Conference on Information Technology (ICIT) (pp. 725-731). IEEE.
[15] ZAMFIROIU, A., POCATILU, P., & CAPISIZU, S. (2019, May). Mobile data vulnerabilities. In Proceedings of the IE 2019 International Conference (pp. 407-412).
[16] Alhashim, S. S., & Rahman, M. H. (2021, July). Cybersecurity Threats in Line with Awareness in Saudi Arabia. In 2021 International Conference on Information Technology (ICIT) (pp. 314-319). IEEE.
[17] Duisebekova, K. S., Sarsenova, Z. N., Pyagay, V. T., Tuyakova, Z. N., Duzbayev, N. T., Aitmagambetov, A. Z., & Amanzholova, S. T. (2019, June). Environmental monitoring system for analysis of climatic and ecological changes using LoRa technology. In Proceedings of the 5th International Conference on Engineering and MIS (pp. 1-6).
[18] Nikkhah, H. R., Balapour, A., & Sabherwal, R. (2018). Mobile applications security: Role of privacy.
[19] Al Jutail, M., Al-Akhras, M., & Albesher, A. (2019). Associated Risks in Mobile Applications Permissions. Journal of Information Security, 10(02), 69.
[20] Koala, G., Bassolé, D., Bissyandé, T. F., & Sié, O. (2019, December). Analysis of the Impact of Permissions on the Vulnerability of Mobile Applications. In International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 3-14). Springer, Cham.
[21] Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone device. International journal of advanced computer science and applications, 7(4), 206-219.
[22] Zeybek, M., Yılmaz, E. N., & Doğru, İ. A. (2019, November). A study on security awareness in mobile devices. In 2019 1st International Informatics and Software Engineering Conference (UBMYK) (pp. 1-6). IEEE.
[23] Abdurachman, E., Gaol, F. L., & Soewito, B. (2019). Survey on threats and risks in the cloud computing environment. Procedia Computer Science, 161, 1325-1332.
[24] Mamun, T. I., & Alam, L. (2016). Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcoming Those Vulnerabilities. International Journal of Computer Applications, 975, 8887.
[25] Bassolé, D., Koala, G., Traoré, Y., & Sié, O. (2020, March). Vulnerability analysis in mobile banking and payment applications on android in African Countries. In International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas (pp. 164-175). Springer, Cham.

Biographies

Sara Alsahaim received a master degree in Cybersecurity from King Faisal University. He has an excellent experience in the cybersecurity field in both theoretical and practical. He has several certificates in cybersecurity like CEH and others. He several publications in cyber risk assessment. His research interests including cyber security, risk assessment and cyber-attacks.

Mohammed Maayah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaayah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain. mohammad7ups@yahoo.com