Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 10, October 2025, pg.50 – 67

Information Security Best Practices to Eliminate Mobile Threats and Attacks

Omaima Nazar A. AlAllaf AlMustawi

Associate Professor, Information Systems Department, College of Computer and Information Sciences,
Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia
onalmustawi@imamu.edu.sa

DOI: https://doi.org/10.47760/ijcsmc.2025.v14i10.005

Abstract: Mobile devices are becoming increasingly common place among users, particularly corporate personnel. The Mobile devices pose a greater danger to corporate security than PCs according to their larger attack surface. Mobiles are used by individuals and enterprises for a variety of purposes including planning and organizing professional life. This led to significantly altering how information systems and Mobile applications are structured, consequently, Cyber Security safeguards all data on Mobiles, other computing and network devices.

Raising awareness about Mobile security threats and recommended practices has become a primary focus due to the continuous emergence of new vulnerabilities in Mobile devices. There is an emergency need to adopt approaches and best practices to secure Mobiles, computing devices and their connected networks to defence against threats and attacks.

To address these significant challenges, this paper aims to identify and describe in details the well-known Mobile threats and attacks. The paper recommends a set of Mobile security best practices that were suggested for Mobile users and organizations to secure their mobile devices against different types of threats and attacks.

Keywords: Phishing Attack, Smishing Attack, Malware, Spyware, Adware/Clickware, Ransomware, Man in the Middle Attack, Clickjacking, Remote Code Execution Vulnerabilities, Data Leakage Threats, Drive-by-Downloads, Unsecured Wi-Fi Networks

I. INTRODUCTION

The number of mobile devices users is continuously rising, and they are increasingly becoming targets of malicious activities related to the distribution of malware-infected applications on Mobiles and other devices running Mobile operating systems (OS) such as Android, iOS and so on. Mobile devices hold photos, document files that contain sensitive information and data [1][2]. Also, the Mobile devices include a lot of applications for human life activities such as bank transactions, E-mails, corporate secrets, digital wallets, social networks messages [3]. The ranges of Mobile devices that are available include Mobile computers, personal digital

assistants/enterprise digital assistants, pagers, personal navigation devices (PNDs), Mobile phones and portable media players [4].

The users of Mobiles and other computing devices are increasingly remaining vulnerable to various types of attacks criminal behaviour in the form of malicious applications being installed on their smartphones. This is done despite the existence of controlled regulated and restricted distribution systems and environments provided by Google and Apple [1]. Therefore, we need to protect this sensitive data by adoption different Mobile security approaches, methods and best practices.

Open Web Application Security Project (OWASP) analysed many Mobile risks according to their top risks list: Improper credential usage; Inadequate supply chain security; Insecure authentication/authorization; Insufficient input/output validation; Insecure communication; Inadequate privacy controls; Insufficient binary protections; Security misconfiguration; Insecure data storage; and finally, Insufficient cryptography. At the same time, the vulnerabilities may consider them in the future: Data leakage; Hardcoded secrets; Insecure access control; Path overwrite and Path traversal; Unprotected endpoints (Deep link, Activity, Service); and Unsafe sharing [5].

Mobile security and security best practices against different threats and malware has become a central objective due to the discovery of new vulnerabilities of mobile devices [6]. Malware can be regarded as one of the numerous security risks that affect mobile devices. It is a malicious software intended to: harm systems; obtain unauthorized access to them; steal data; or interfere with device operation. It can take advantage of flaws in applications and OS and frequently targets Mobile cloud services. Malware that steals credentials, OS flaws, app flaws, and intrusive user tracking are common risks to Mobile security [7].

- **Phishing:** is the term for unsecure attempts to obtain private information through Mobile phone communications, usually sent by SMS or email [8].
- **Unauthorized Access**: Risks associated with insufficient authentication procedures that may lead to breaches of financial and personal data [9].
- **Communication attacks**: When data is intercepted or modified during transmission. Supply chain attacks: Vulnerabilities can be introduced into the Mobile ecosystem through third-party apps or services [8].
- **Physical Attacks**: Attacks that are directed at the device itself.
- **Authentication Attacks**: Attempts to bypass security mechanisms that verify a user's identity [1].

Significant data breaches and financial losses may result from these various attacks [7][8]. Understanding these risks and putting appropriate preventative measures in place are essential for both users and enterprises as Mobile technology develops further. To prevent these risks, we must talk about the current threats as well as hacking techniques and how they operate.

According to literature studies related to Mobile security, there is a shortage in studies related to describing in details the different types of well-known Mobile threats and attacks that face Mobile users. Therefore, this paper aims to list and describe the well-known Mobile security threats and attacks that face people in different society sectors and enterprises. This paper focuses also on identifying the Mobile security best practices that are recommended for protecting and securing Mobile devices. The paper is organized as follows: Section II includes overview of related literature studies. Section III presents the different types of Mobile threats, risks and attacks. The comparison between many Mobile threats and attacks will be considered in section IV. Section V includes the recommended best practices that were suggested for Mobile security. The conclusion of this work will be included in section VII.

II. RELATED STUDIES

Mobile devices have grown significantly in recent years compared to desktop computers. The rise in Mobile device usage provides hackers with many opportunities to steal confidential information or conduct other types of attacks on these devices. This section reviews the literature studies related to common Mobile security threats and hacking techniques that affect Mobile devices. Weichbroth and Łysik (2020) [1] carried out a literature study on Mobile security threats and their defences. They addressed also the dangers of social and physical causes. According to their analysis of studies related to Mobile best practices, they suggested to use built-in techniques to reduce the harmful effects of hostile SW and social engineering frauds. And, Nagarjun and Shaik (2018) [3] investigated many security threats associated with Mobile apps and devices. They addressed a number of protective strategies to stop these Mobile security threats.

Whereas, Kevin Curran et al. (2015) [4] emphasized the security measures put in place to ensure that Mobile devices are secure to use. Some examples of these measures are: The users' selection of the Mobile devices, encryption, authentication, remote wiping, firewalls, lost phone hotlines, third-party software, intrusion prevention software, anti-virus software, and Bluetooth. In the same year, Ibrahim et al. (2015) [6] highlighted Mobile phone security and recommendations for Mobile security. On the other hand, Ilapakurthy (2023) [7] analysed the most significant Mobile security issues, such as:

- Vulnerabilities in Mobile applications that facilitate attacks;
- Growing privacy risks for users caused by excessive tracking;

- Low-level OS and HW vulnerabilities that enable attacks on the confidentiality and integrity of Mobile cloud systems; and finally,
- Malware that steals credentials and data from Mobile cloud services.

He went over the existing security flaws, including: fragmented visibility throughout the Mobile ecosystem; coarse-grained access control; and Malware detection based on signatures. He discussed also the preventative techniques like formal verification, HW anchored security, intelligence-driven Malware adaptation, integrated cross-layer security, and the importance of robust security foundations for Mobile cloud computing to improve the overall Mobile security.

A summary of the various Mobile security attacks and threats was given by Marc Schmitt (2022) [8]. He underlined the cyber threats, which the world economic forum has identified as a major global security problem are increasingly targeting Mobile devices [8]. He recommended putting strong security measures in place to counter these threats, like: Frequent SW upgrades to fix vulnerabilities; employee education to spot phishing efforts; and powerful authentication techniques to protect access. Additionally, Mona Adlakha (2016) [9] discussed common Mobile security risks such as: Malware, illegal access, and transactions that aren't authenticated. She implemented a number of risk prevention techniques related to Mobile financial transactions, including:

- Implementing digital and physical security measures;
- Conducting independent compliance audits; and
- Regularly reviewing and updating security plans to address new issues.

Theft of personal information, user tracking, and malicious activities due to device resource limitations are common Mobile security issues. Daghmehchi, Arash and Fitriah (2024) [10] highlighted the significance of Mobile application security, and provided security best practices to reduce security threats. This is accomplished by employing secure coding practices and making sure that users and app developers have strong infrastructure-related security protections in place.

Policies that prevent data leaks are crucial for Mobile security and businesses must implement adaptable security guidelines for individual devices. Won Hyung Park, et al. (2013) [11] covered common Mobile security risks such as: Malware infections; data leaks; and unauthorized access. They recommended the use of preventative techniques by putting Mobile device management, Mobile application management, and strong mobile security rules into place to safeguard sensitive data and monitor device security. And Teodor Mitrea and Monica Borda (2020) [12] discussed numerous mobile security risks, including viruses, data leaks, and unauthorized access. They recommended several preventative measures such as: the use of encryption; the implementation of two-factor authentication; network traffic monitoring; the blocking of superfluous internet access; and the use of SSL/TLS protocols to ensure secure client-server communications. In contrast, Timothy Speed et al. (2013) [13] discussed common dangers to Mobile security, such as Malware, Hacking, and data theft. To prevent these risks, they recommended: using two-factor authentication, creating strong passwords, updating SW, avoiding important transactions on public Wi-Fi, and routinely backing up data to recover from possible breaches.

Stakeholder cooperation is necessary for Mobile malware detection. Additionally, promising Mobile security solutions are provided via cloud-based detection. Numerous Mobile security risks, including drive-by downloads, privilege escalation, and repackaged apps, were discussed by Nicholas Penning, et. al (2014) [14]. In order to reduce the dangers connected with Mobile Malware, prevention techniques include the use of cloud-based detection frameworks, static and dynamic analysis, and user education regarding safe app practices.

From the above researches review, there is a shortage in researches and articles that describe in details the different types of Mobile security attacks that face mobile users and harm Mobiles and other computing devices. Therefore, section III lists and describes the well-known Mobile security attacks and provide in details their types and effects.

III. MOBILE ATTACKS AND THREATS

Mobile devices are particularly vulnerable to different security threats due to the sensitive financial and personal data they store. This includes risks from Malware, Spyware, and unauthorized access, which can lead to significant financial losses and breaches of privacy. All the majority of Mobile threats and attacks are covered in this section.

A. Fishing Attack

Phishing is a common and dangerous cyberattack designed to deceive users into revealing sensitive information. It affects individuals, organizations, and companies. Attackers employ various methods, such as creating fake emails, using social engineering tactics, or directing users to fraudulent websites. Targeted phishing methods, like spear Phishing and whaling, customize messages for specific individuals or notable targets. Consequences of phishing attacks include financial loss, identity theft, damage to reputation, and

breaches of critical systems. One method used to gather information is Phishing. Phishing is a type of cybercrime that focuses on emails, phone calls, text messages, passwords, banking details, credit card numbers, and personal identifying information. It is mainly a tactic for online identity theft. Attackers use social engineering to acquire the victim's account and personal information [15].

Phishing is the act of attempting to obtain personal information, such as credit card numbers, usernames, and passwords, by pretending to be a trustworthy entity through electronic messages. People are often deceived by messages that appear to come from popular social media sites, auction platforms, online payment services, or IT administrators. Phishing emails may contain links to malicious websites [16][17]. One type of social engineering is Phishing. Phishing is mainly used in email hacking, where the hacker sends a link via email to the user, asking for, for example, bank account details or other personal information. The user clicks the link and fills in the requested information, giving the hacker access to all their data. Phishing steps are [15]:

1. The attacker sends an email to the victim.
2. When the victim clicks on the email, they are directed to a phishing website.
3. The attacker captures the victim's login credentials.
4. The attacker uses the victim's login credentials to access a website.

Phishing begins with an email or other form of communication intended to aid in the victim's attack. The communication is presented as though it were sent by a reliable source. The victim is giving their personal information to a spam website if they fall for it. Malware can occasionally be downloaded into the target PC as well. Phishing is carried out in this manner as seen in Fig.1 [15].

Phishing attacks can now be executed using increasingly sophisticated techniques, such as spear phishing, whaling, clone phishing, vishing, smishing, and search engine phishing, in addition to traditional email phishing. Muhammad Nadeem et al. (2023) [16] provided a comprehensive analysis of phishing attacks, including their history, methodologies, impacts, and countermeasures. By thoroughly reviewing numerous case studies, they highlighted the substantial financial and non-financial consequences of these attacks. They also stressed the importance of ongoing research and technological advancements while pointing out emerging challenges.

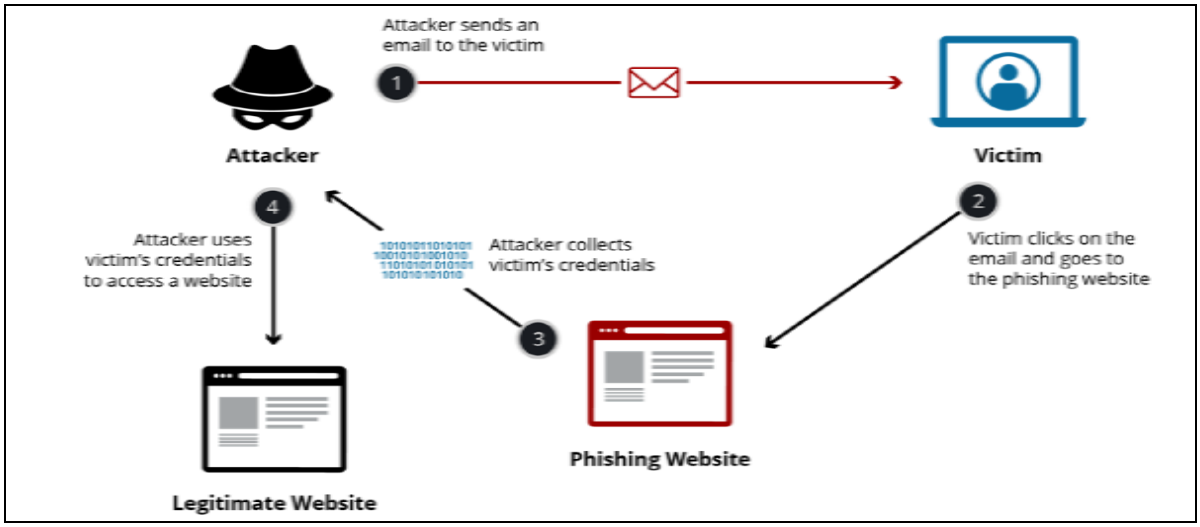


Fig.1: Fishing Attack [15]

Phishing attacks are malicious efforts to deceive individuals into revealing private information by pretending to be trustworthy organizations. To effectively combat these threats, new detection and prevention methods have recently been developed. Two methods had been used to detect Phishing attacks: the first one is **Directional Phishing Detection**, that analyse the user network access data to identify suspicious login patterns and estimates the likelihood of a Phishing attack. This is done by comparing the login page's characteristics to known legitimate configurations [17]. The second method is **Heuristic Techniques**, where various heuristic methods are employed to detect and prevent Phishing attempts, particularly in Mobile environments [18]. In contrast, the following are the prevention strategies:

- **Client Blacklisting**: Keeping a list of clients to block is an approach to prevent registration attempts from known Phishing websites and reduce resource losses [19].
- **Graphical Two-Dimensional Codes**: Requiring verification on both PC and Mobile devices, the use of dual-link data for authentication enhances security [20].
- **Trusted Computing**: Reviewing current preventive methods shows that integrating SSL protocols with trusted computing technology effectively stops Phishing attacks [21].

Even though these techniques greatly improve security, the dynamic nature of Phishing techniques demands constant innovation and adaptation in detection and prevention techniques.

B. Smishing Attack

Smishing is a social engineering technique that uses fraudulent text messages on Mobile phones to deceive people into installing malicious software, sharing personal information, or transferring money to online scammers. The term "Smishing" is a blend of Phishing and short message service (SMS) for text messaging. By combining SMS and Phishing, Smishing describes the use of text messaging technology along with the deceptive strategies commonly associated with Phishing attacks [22][23].

A number of reasons have contributed to the rise of Smishing. Firstly, hackers, often called Smishers, know that people are more likely to respond to text messages than to other forms of communication, making them prime targets for exploitation. Additionally, advancements in spam filters and security measures for phones and emails have made traditional Phishing attacks less effective, prompting attackers to focus on smishing as an alternative method [24]. Fig.2 illustrates the phases of Smishing attack [23]. The increasing prevalence of this form of social engineering necessitates sophisticated detection techniques to protect both consumers and organizations.

Smishing mechanisms such as sending SMS messages containing malicious URLs or requests for personal information is a common tactic in Smishing attacks [25]. To persuade victims to click on links or reveal private information, attackers often create a sense of urgency or trust [26].

Neural networks (NN) and decision Trees are two examples of machine learning (ML) algorithms that have been successfully used to detect Smishing communications [26]. High accuracy rates in Smishing detection have been shown in recent studies and some algorithms have achieved above 97% accuracy [25].

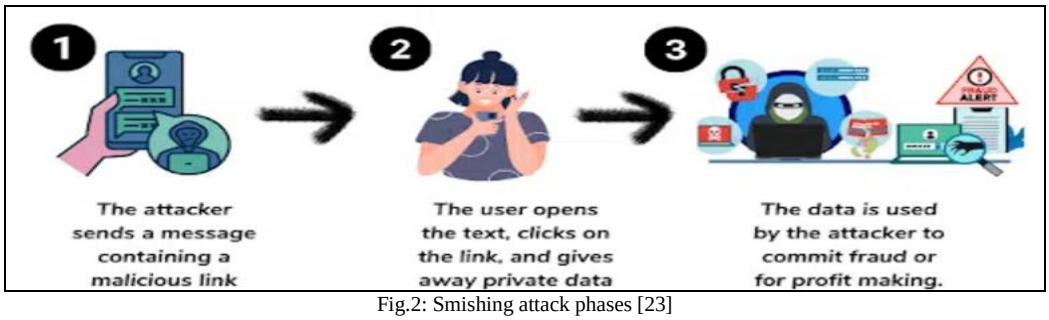


Fig.2: Smishing attack phases [23]

It is essential to teach people about Smishing techniques, however this is a difficult task because Smishing attacks are constantly changing [26]. While ongoing awareness programs can help reduce hazards, strong defense requires technology solutions [27]. The dynamic nature of Smishing tactics needs continuous user education and adaptive security measures to offer comprehensive protection against this changing danger, even while technology breakthroughs in detection show promise.

C. Malware

As Mobile phone capabilities continue to evolve, Malware poses a significant threat as it provides hackers with incentives similar to those found in PC systems. These incentives include fraud and the theft of personal and corporate data. Hackers can spread Malware and carry out harmful actions through various methods due to the ever-changing mobile technology landscape [1].

It is expected that several factors such as: the evolution of Malware techniques; the increasing number of Mobile devices; and vulnerabilities in Mobile communication technologies, will influence the global spread of Mobile Malware. As Mobile Malware becomes more sophisticated, it is likely to spread more broadly, placing individuals at serious risk worldwide. **Colluding Apps** can be regarded as one of the development Malware methods, whereas new risks arise, harmful operations are carried out by apps working together, making detection difficult [28]. The other development Malware method is **Behavioral Patterns** in which Mobile Malware has general tendencies that are exploitable, which calls for sophisticated detection techniques [29]. There are two vulnerabilities in communication technologies: Exploits for messaging and Bluetooth; and proximity-based spread. In **Exploits for messaging and Bluetooth**, the proliferation of Bluetooth and Mobile messaging has made it possible for malware to propagate quickly, especially via SMS and MMS channels [30]. While in **proximity-based spread**, the Monte Carlo simulations have demonstrated that malware can use proximity technologies, such as Bluetooth and NFC, to infect devices [31].

It is anticipated that Mobile Malware would be more expensive and destructive than conventional PC infections, underscoring the pressing need for efficient defenses [29]. Also, teaching users about the dangers of Mobile Malware and how to avoid it is becoming more and more important [32]. On the other hand, even if Mobile

Malware poses a serious concern, some risks may be reduced by improvements in detection technologies and user education. To keep abreast of changing threats, cybersecurity research and development must be ongoing.

- **Malware Instances**

1) Spyware:

A program that collects statistical data from a user's Mobile device and sends it over the internet without the user's permission. This data is usually gathered from cookies and the browsing history of the Mobile device. Besides collecting data, Mobile Spyware can also install additional software, show unwanted ads, or redirect the user's browsing activities. Due to their ability to secretly gather personal information, spyware attacks represent a significant cybersecurity threat. Examples of Spyware: Trojan horses and Keyloggers, which exploit system vulnerabilities to obtain data without user consent. There are three Attack mechanisms for Spyware:

Trojan Horses: are programs that pose as trustworthy apps to obtain private information from Mobile devices, including contacts, SMS, and Call logs, without the user's knowledge [35]. Mwange & Cankaya (2024) [35] discussed the new Trojan horse Spyware for Android that may covertly collect private information such as contacts, SMSs, and phone logs. It can also be used to execute DDoS assaults on certain IP addresses and enable remote control for cyber espionage. They recommended design to raise awareness and strengthen Android security. A Trojan can carry out a number of harmful tasks after infiltrating a device such as: creating a backdoor for unwanted access; obtaining root or jailbreak privileges; spying or recording keystrokes; and spreading botnets to launch Distributed Denial of Service (DDoS) attacks [8].

Keyloggers: A serious risk during sensitive transactions. This kind of Spyware logs keystrokes and stores them in log files that are delivered to malevolent individuals [36]. Spyware that uses keyloggers is very dangerous for systems that are utilized for everyday transactions. The Spyware emails this log file to the malicious user once the keylogger logs the system user's keystrokes and saves them in a log file. Therefore, Akhil, Neeraja, and Arun (2014) [36] presented a technique for identifying and averting keylogger Spyware attacks.

Zero-click Exploits (Pegasus spyware): Pegasus and other advanced spyware may sneak into systems without requiring any user involvement by using zero-day flaws to extract data. It works secretly by sneaking into target computers without the user's awareness, gathering private data, and keeping an eye on user activity. Because of its limited traceability, strong surveillance capabilities, and covert infiltration, the Pegasus spyware poses a serious cybersecurity risk. Innovative methods to identify and stop its deployment are necessary for mitigating this hazard [37]. In order to protect systems and user privacy, Sidhant Chourasiya et al. (2023) [37] offered insightful information about how Pegasus functions and paved the way for the creation of practical countermeasures and mitigation techniques. They looked at the peculiarities and consequences of the Pegasus spyware. Its zero-click functionality, in which exploitation takes place without user intervention, and its dependence on zero-day vulnerabilities for system compromise are specifically understood. They also investigated how much control the Pegasus operator was given, including the ability to execute commands, view data, and remotely modify HW components.

They thoroughly investigated the technical complexities of the Pegasus spyware. They also looked at Pegasus's propagation strategies, highlighting how it can take advantage of zero-day vulnerabilities without requiring user interaction. Additionally, methods used by malware to create command and control channels are examined through HTTPS connections, opening up possible tracking and detection paths. According to their results, Pegasus is evasive and leaves very little evidence of its activity on compromised systems. It is quite difficult to identify and follow the program because of its complex methods and dependence on encrypted communication connections. They also emphasized how the Pegasus operator was given a great deal of control, which allowed for thorough monitoring and data exfiltration from infiltrated systems [37].

Biometric Authentication can significantly reduce the success rate of impersonation attacks like Spyware. It is an enhancement to traditional password systems such as incorporating biometric data [38]. Ajith, Manikandan, and Sheela (2024) [38] proposed incorporating biometric information as an additional layer of user authentication to improve the current authentication systems that rely on one-time passwords (OTP) and personal identification numbers (PIN). Instead of typing the password as usual, users who follow the suggested way sketch each digit on the device's touchscreen. They carried out a thorough analysis of the resilience and discriminative power of each handwritten digit in addition to a performance evaluation of their suggested biometric technique with longer passwords. They used finger input on a Mobile to generate e-BioDigit database, which consists of handwritten numbers 0 through 9. Positive results have been obtained from their application to improve the security of the current PIN and OTP systems. In particular, this technique exhibits equal mistake rates of roughly 4.0% in situations where the attacker already knows the password. In contrast, an impersonation attack would always be successful in 100% of circumstances with classic PIN and OTP systems [38].

Graphical CAPTCHAs can be used also to reduce the success rate of impersonation Spyware attacks. This is done by storing user inputs in a non-text format that is more difficult for Malware to decipher, click-based graphical CAPTCHAs can prevent keyloggers [39]. To overcome the Spyware attacks, Bindu (2015) [39] suggested a click-based Graphical CAPTCHA. When using a standard text-based CAPTCHA, the user often

inputs random characters to create a CAPTCHA, which are then saved in key loggers for easy decoding by spyware. Click-based Graphical CAPTCHA employs a special verification method in which the user clicks on a series of images to create a CAPTCHA. The sequence is saved in pixels with a predetermined, random order. He examined the suggested plan's performance, security, and usability. Despite the potential of these remedies, spyware's dynamic nature demands constant innovation in detection and prevention techniques to protect user privacy and data integrity.

2) Adware/Clickware:

Adware, sometimes referred to as advertising-supported software, is a category of harmful software that frequently jeopardizes user privacy and experience by displaying unsolicited advertisements on a user's computer. It usually takes the form of pop-up windows or banner advertising, and its main objective is to make money for the offender by getting clicks or ad impressions. The traits, effects, and detection techniques of adware are covered in further detail in the sections that follow. Adware can cause click fraud and other harmful actions by entering devices and presenting unwanted adverts [40]. Adware bombards consumers with too many advertisements, which reduces the device's overall usefulness and may result in further security flaws [40]. Adware affects two things: privacy risks and monetization. Adware is a profitable channel for cybercriminals since it can be a component of a larger plan to monetise false ad traffic [41]. However, because adware frequently gathers information about user behavior in order to customize ads, its presence can expose users to privacy risks.

AI driven solutions can be used as an Adware detection method. This is done by examining user behavior and spotting patterns suggestive of adware presence, recent developments in artificial intelligence have demonstrated promise in adware detection [40].

Whereas, Adware preventive methods to lessen the impact of Adware are being developed, including tracking network access requests and intercepting harmful marketing URLs [42]. Although Adware presents serious concerns, it's important to remember that not all software that uses ads is harmful; some programs use advertising as a valid source of income. However, it might be difficult to distinguish between malicious and lawful adware, therefore effective detection and prevention techniques are required [42][43].

3) Android GMBot:

The phrase "Android GMBot" can be used to describe a variety of robots and apps that use Android technology for control and automation. This includes Android application-controlled robots and tools for automating tasks on Android devices.

- **DroidBot-GPT: Automation on Android**

  DroidBot-GPT converts user tasks into executable actions by automating interactions with Android apps using models similar to GPT [44]. There is room for improvement in automation performance, as evidenced by its 39.39% job completion rate across 33 tasks from 17 applications [44].

- **Agricultural Robotics**

  With the help of an Android app and Bluetooth, a mobile robot with Android that is intended for agricultural work can carry out duties like seeding and plowing [45]. This robot demonstrates the usefulness of Android technology in agriculture by attempting to increase productivity and decrease labor in farming [45].

- **Voice-Controlled Robotics**

  Using Google's Speech API for real-time command processing, an Android-based application enables users to manage a mobile robot with voice commands [46]. Voice recognition improves accessibility and user involvement in robotic control [46]. Although these apps demonstrate Android's adaptability in automation and robotics, there are still issues with increasing task completion rates and guaranteeing dependability in a variety of settings.

4) AceDeceiver iOS Malware:

AceDeceiver is one of the well-known iOS Malware that represents the changing threat landscape aimed at Apple devices. This Malware disseminated through unofficial means and mainly takes advantage of flaws in jailbroken iOS systems, and emphasizes the necessity of strong security measures.

AceDeceiver is made to pose as trustworthy software to trick users into installing harmful apps. Because jailbroken devices have different security settings, they are more vulnerable to malware [47]. By using social engineering techniques, the Malware can install other harmful apps without the user's permission [48].

Unofficial channels and Exploiting development tools represent the *d*istribution methods of the AceDeceiver iOS Malware**. In unofficial channels**, the AceDeceiver frequently gets over Apple's rigorous software Store review process by being downloaded through file-sharing sites and third-party software shops [49]. Whereas in **Exploiting development tools**, the Malware has been embedded in legitimate applications by attackers who have compromised development tools like as Xcode [49].

AceDeceiver and other iOS viruses have become more prevalent, indicating a shift in focus from Android to iOS and the need for stronger security measures [47][48]. To reduce potential risks, users should be informed about the dangers of jailbreaking and obtaining apps from unapproved sources.
Even though AceDeceiver poses a serious risk, it also emphasizes how crucial it is to continue researching and developing mobile security. To keep iOS a safe platform for consumers, anti-malware techniques must also change as malware tactics do.

5) Ransomware:
Because of its capacity to encrypt data and demand ransom payments, frequently in cryptocurrency, ransomware has become a serious danger in the realm of cybercrime. Ransomware, which started out targeting individuals, has now turned its attention to organizations, resulting in significant financial demands and the emergence of ransomware-as-a-service models. Improved cybersecurity measures are now required in many industries, especially those that are vital to infrastructure, as a result of this evolution.
With modest ransom demands, ransomware first affected residential users in the late 2000s [50]. Attacks on organizations increased in frequency by the 2020s, and ransom demands topped $1 million [50]. The serious operational effects of ransomware are demonstrated by well-known events like the Colonial Pipeline attack [51]. Critical cyber-physical systems are among the many users that ransomware targets [52]. These attacks heavily rely on social engineering, which uses psychological cues to obtain access [52]. Because they depend on interconnected networks, certain industries, such as healthcare and energy, are especially vulnerable [53].
Effective detection techniques are crucial; new research has produced algorithms that can identify ransomware threats with over 99% accuracy [53]. Businesses are urged to implement multi-layered cybersecurity plans that integrate cutting-edge technology with human attention to detail [51]. To reduce hazards, it is essential to invest in safe protocols and network security [54]. Although ransomware is a serious concern, some contend that the likelihood of such attacks may be successfully decreased with greater knowledge and better cybersecurity measures. These safeguards are still put to the test, though, because ransomware techniques are always changing.

D. Man in the Middle Attack (MITM):
MITM attacks represent serious risks to digital communication because they enable attackers to secretly intercept and alter data between two parties. Due to the difficulty of identifying these attacks, numerous cutting-edge detection and protection techniques have been developed.
A hostile actor placing themselves between a user and an application to mimic the communication. The goal of this assault is to steal personal data, including credit card numbers, account information, and login credentials. By installing malicious Wi-Fi hotspots or changing network protocols, the attacker can intercept traffic in a number of ways. The attacker may decrypt and access private information after intercepting the traffic without the user's knowledge. Fig.3 illustrates the MITM attack.
MITM attacks can be avoided by utilizing secure communication protocols like TLS and HTTPS, exercising caution when using unprotected networks, and putting robust encryption and authentication procedures in place.
Imperva provides security services that guard against MITM attacks and optimize SSL/TLS encryption [55]. Iddrisu et al (2024) [56] demonstrated in their study an approach based on Convolutional Neural Networks (CNNs) to detect the MITM attack. They achieved a detection accuracy of 98.6% that shows the effectiveness of deep learning in identifying MITM attacks. While, Rao et al (2024) [57] utilized machine learning to predict potential MITM attacks by analyzing network data and enhancing proactive security measures.
At the same time, many other literature studies where focused on MITM attack prevention strategies. Mwakajwanga and Mwambe (2024) [58] proposed a hybrid approach combining image steganography, AES encryption, and digital signatures to secure data against MITM attacks. They proved an effectiveness in maintaining message confidentiality
Whereas, Thankappan et al (2024) [59] developed a distributed system based on signature intrusion detection to monitor and detect multi-channel MITM attacks in Wi-Fi networks. They achieved average detection accuracy equal 98%. While these advancements significantly improve security against MITM attacks, challenges remain, particularly in adapting existing systems to new attack vectors and ensuring comprehensive protection across diverse environments.

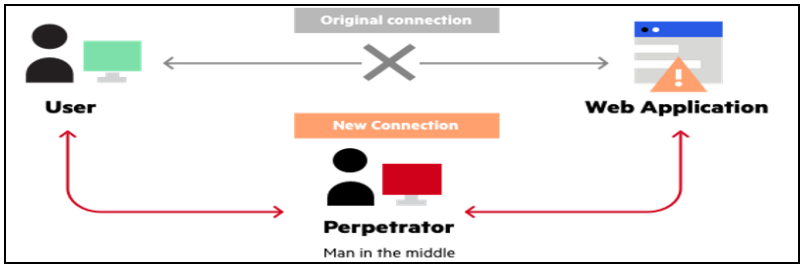


Fig.3: MITM attack [55]

E. Clickjacking

Clickjacking is a sophisticated online security threat that deceive users into clicking on hidden buttons or links by superimposing transparent elements over trustworthy websites. This attack takes advantage of flaws in site architecture and may result in illegal activities like data theft or unsolicited posts. Examining clickjacking's mechanics, detection techniques, and defenses is necessary to comprehend it. The act of a malicious website hiding sensitive user interface elements by overlapping web frames and making them invisible to the user is known as "clickjacking" [60]. Attackers can get private information, such as location and mobile numbers, by utilizing deceptive links.

Various detection methods with simulation click operations have been developed to identify vulnerabilities in web pages [61]. To combat the clickjacking threat, Kavitha and Ravikumar (2015) [61] offered a security measure called a whitelisting URL analyzer. With regard to the application context in the social networking environment, their security mechanism has the capacity to quantify the assault and the extent to which the vulnerability is being exposed.

Their suggested DNSlookup and iframe tag detection algorithms are based on regex. Using straightforward regex patterns, regex effectively manages both internal and external faults and shortens the load time of DNSlookup and iframe tag inspection. The difference between the system state and the intended state can be used to gauge the attack's vulnerability. The security mechanism can overcome this deviation [61].

On the other hand, Aryaman et al. (2023) [60] offered efficient defenses, such as the use of server-side security headers like content-security-policy and X-Frame-Options.

Advanced methods, such the Extreme Learning Machine algorithm, were created by Yashodha Patil (2020) [62] to categorize and detect harmful links linked to clickjacking. Even though clickjacking is extremely dangerous, creating strong defenses requires constant research and technology development. However, due to the dynamic nature of online threats, security measures must be continuously monitored and adjusted.

F. Remote Code Execution (RCE) Vulnerabilities

RCE vulnerabilities represent serious risks to digital infrastructures. This is because they enable attackers to run arbitrary code on a target system. Unauthorized access to private data, service interruptions, and data breaches can result from these vulnerabilities. From web applications to cross-platform ecosystems, the intricacy and consequences of RCE vulnerabilities are apparent in a variety of settings. The processes, detection methods, and mitigation techniques for RCE vulnerabilities are examined in the sections that follow. Three mechanisms of RCE vulnerabilities

CVE-2023-33246: This Apache RocketMQ vulnerability illustrates how RCE can disrupt services and compromise data. Making the broker filter server module optional and implementing multi-layer protections can reduce the risk of exploitation [63].

LLM-Integrated programs: Prompt injection is often the source of RCE vulnerabilities in these programs, enabling attackers to execute code remotely. A thorough study identified twelve RCE vulnerabilities across various frameworks [64]. Fig.4 shows the basic workflow of LLM-Integrated web application involving code execution.

Cross-Platform Ecosystems: XRCE attacks, often caused by XSS or untrusted data, can impact JavaScript frameworks. On local devices, these attacks can execute malicious code [65].

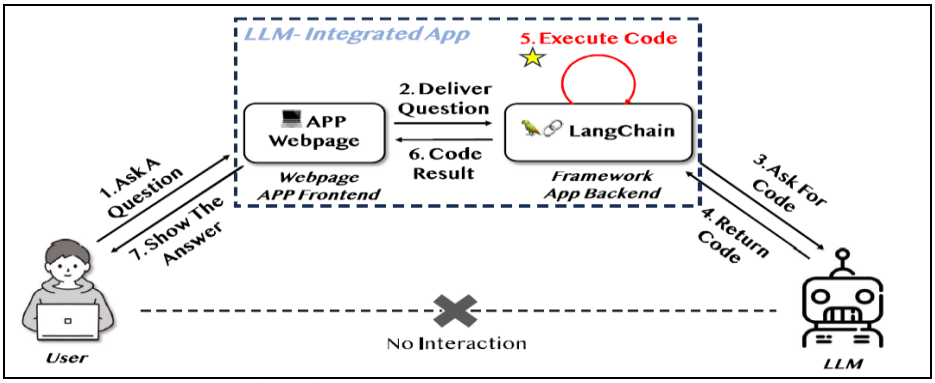


Fig.4: Simple workflow of LLM-Integrated web application involving code execution [64]

The packet content-oriented detection can be used to detect the RCE vulnerabilities. In this method, a packet content-oriented detection model has been developed that focuses on attacks against XML External Entity, Expression Language Injection, and Insecure Deserialization. Sun et al. (2024) [66] used ML to detect RCE payloads with high recall and accuracy.

The static analysis and automated testing can be used also to detect RCE vulnerabilities**.** While prompt-based testing confirms vulnerabilities in real-world situations, Liu et al., (2023) [64] used tools such as LLMSmith search source code for possible RCE vulnerabilities.

One of the RCE mitigation strategies is to use an enhanced architecture. This is done by adding multi-layer message validation, access control, and anomaly detection to Apache RocketMQ. This can successfully prevent RCE without sacrificing performance [63].

Another RCE mitigation strategies is to use XGuard technology. This is done by addressing the characteristics and attack surfaces of XRCE variants. Then this can automatically mitigates RCE [65].

Even though RCE vulnerabilities pose serious threats, improving security requires constant study and development of detection and mitigation techniques. The combination of automated techniques and machine learning models presents promising ways to find and fix these vulnerabilities. To protect digital infrastructures, security measures must be continuously improved and adjusted due to the dynamic nature of RCE threats.

G. Data Leakage Threats

Data Leakage poses serious risks in many fields especially in federated learning, cybersecurity, and machine learning. It involves unauthorized exposure of private data, which can lead to severe consequences for organizations. Developing successful prevention and detection measures requires an understanding of the mechanics and consequences of data leaking [67]. Data Leakage threats come in three different types: Federated Learning Risks, Insider Threats, and Machine Learning Preprocessing.

Federated Learning Risks: Data leakage can occur during federated training, where training data privacy may be compromised through gradient updates. Wei et al. (2024) [67] conducted Mitigation strategies including adding randomized noise to gradient updates.

Insider Threats: Malicious activities by authorized members can lead to data leakage, necessitating robust detection methods. Wang et al. (2024) [68] suggested technique like Cyclical Learning Rate based Long-Short Term Memory (CLR based LSTM). This technique had shown high accuracy in recognizing such behaviours.

Machine Learning Preprocessing: Data leakage during preprocessing skews model performance, leading to misleading metrics. Bouke et al. (2024) [69] showed in their study significant performance discrepancies across various datasets due to leakage.

Data Leakage Prevention (DLP) can be used to prevent the Data Leakage threats. Where the organizations are increasingly adopting DLP techniques to safeguard against unauthorized access and insider threats. This method focus on monitoring data flow and implementing proactive measures. Syarova et al., (2024) [70] explored the DLP and detection techniques as some of the most critical cybersecurity issues nowadays. Sultan Alneyadi, et. al (2015) [71] carried out a comprehensive survey on the current DLP systems mechanisms. They categorised the active research directions in DLP field. Also they suggested future directions towards developing more consistent DLP systems that can overcome some limitations of the current ones.

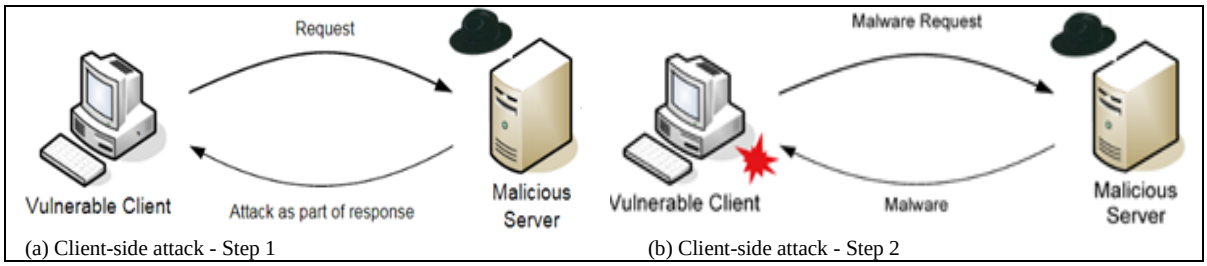
Comprehensive assessments of Data Leakage vulnerabilities can help organizations identify and mitigate risks effectively. Periasamy J K, et. al (2023) [72] presented a comprehensive exploration into Data Leakage analysis including methodologies, case studies, and emerging technologies in Data Leakage analysis. They aimed to enhance understanding, detection, and mitigation of data leakage risks. They suggested best practices that are essential for enhancing data security, minimize vulnerabilities, and enable proactive measures in mitigating potential data breaches.

Although the focus on data leakage prevention is critical, it is important also to recognize that not all data exposure is malicious. In many cases, data sharing can lead to beneficial outcomes, such as improved model performance through collaborative learning. Balancing security with innovation remains a challenge in the digital landscape.

H. Drive-by-Downloads Attack

Drive-by-downloads are a specific type of client-side attacks. Primarily, these drive-by-downloads are launched in the context of web browsing. In such a scenario, as shown in Fig.5, a web browser requests web pages from a remote web server.

As a response, the server returns a web page to the web browser, which contains attack code that exploits a web browser vulnerability (Step 1). Once the attack has been successful, malware is pushed or downloaded to and executed on the local workstation without the user's consent or notice (Step 2) [73].



(a) Client-side attack - Step 1 (b) Client-side attack - Step 2

Fig.5: Drive-by-Downloads Attack [73]

I. Unsecured Wi-Fi Networks

One of the primary signs of an unsecured network is the absence of password protection. When a network lacks a password, anyone within range can connect to it without any authentication. This leaves your network open to potential intruders who can gain unauthorized access to your sensitive information [74]. Unsecured networks include public networks, school networks, and similar types. Once access is gained, attackers can retrieve information from all devices connected to the local area network, similar to the hazards of piggybacking. Significantly, large-scale victims of wardriving attacks often consist of public networks and home networks without password protection [75].

Most routers have encryption turned off by default, so it needs to be activated during the network setup. If a computer expert installs the network, it's likely that encryption will be enabled. However, there's no definite way to be certain… Without encryption, any data you send through the router is completely exposed. The most security risks of public WiFi networks are: MITM, Sniffing (or snooping/eavesdropping), Rogue hotspots (or evil twin/honeypot), and Malware injection.

MITM attack: it is the frequent danger on unsecured Wi-Fi networks. When your device accesses the Internet, it communicates with web servers, and security gaps can let a hacker capture your data without you realizing it. You might think you're interacting directly with a website through your router, but the hacker is intercepting and potentially modifying your messages. Essentially, you are only seeing the information that the hacker chooses to send back to you.

Sniffing attack: Cybercriminals can also use specialized software or hardware to intercept and record traffic on a WiFi network. As data moves through the network, the sniffer (or snooper) captures each packet and analyzes its contents. Again, this is an invisible attack. This method enables hackers to monitor all your online activities: see the websites you visit, steal your login information, and even compromise your account. Fig.6 shows the steps of the Sniffing (or snooping/eavesdropping) attack [76].

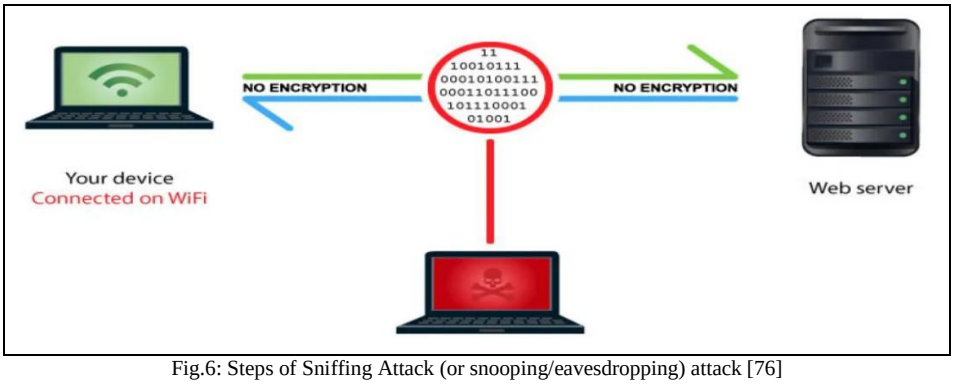


Fig.6: Steps of Sniffing Attack (or snooping/eavesdropping) attack [76]

Rogue hotspots: are unsecured WiFi networks that look legitimate because of their trustworthy names, like Library or Cafe. However, they are actually set up by hackers. If you connect to a rogue network without realizing it, the hacker can carry out attacks and capture all your data. You never really know who is operating an unsecured WiFi network—it might be a 12-year-old using free hacking tools, or it could be something far more serious.

Malware Insertion: vulnerabilities in SW let attackers place harmful programs on your computer. This malware remains concealed until it is too late. Typically, hackers take advantage of security gaps or weaknesses in your operating system (OS) or any application you have installed. Once they gain access to your device, they can easily conduct a MITM attack and reach all of your data [76].

IV. COMPARISONS BETWEEN MOBILE THREATS AND ATTACKS

Mobiles and other computing devices are commonly used for both personal and business activities. These devices often store sensitive information, making them attractive targets for cybercriminals. Therefore, ensuring mobile security is crucial. Different types of mobile threats and attacks were discussed in details in section III. Each one of these attacks types has its own target, delivery method, intent, behaviour, detection difficulty and prevention method. Table I shows the differences between different famous types of mobile threats and attacks.

Mobile security testing aims to identify vulnerabilities and harmful applications on mobile devices. However, the benefits of Mobile security can be summarized by following [77]:

Data Protection: Mobile security protects device passwords, financial information, and personal data.

Malware Defense: Mobile security helps prevent infections by blocking harmful apps and attacks.

Privacy Protection: Mobile security prevents unauthorized access, safeguarding the privacy of communications and data.

Vulnerability Detection: Testing methods detect flaws in apps and devices for timely resolution.

Threat Mitigation: Mobile security mitigates/reduces cyber threats by blocking malware, sniffers, spam, and phishing.

Transaction Security: Protocols ensure secure mobile banking and shopping by maintaining data integrity.

In contrast, Mobile security also has several drawbacks [78]:

- Many safety measures and procedures can be cumbersome and confusing for users.
- Antivirus and security software may slow down computer performance.
- Background monitoring and security applications might drain the battery faster and require more frequent charging.
- Access to certain features or apps may be restricted depending on your device and operating system.
- Many advanced security systems require paid subscriptions, which might be a barrier for budget-conscious users and could affect their online safety.

TABLE I
COMPARISONS BETWEEN DIFFERENT TYPES OF THREATS AND ATTACKS

Attack Type	Target	Delivery Method	Intent	Technical Skill	Detection Difficulty	Prevention Tips
Phishing	Email	Email	Steal Credentials, Personal Information	Low	Moderate	Use strong passwords, be cautious with attachments, verify sender
Smishing	SMS	SMS	Steal Credentials, Personal Information	Low	Moderate	Use strong passwords, be cautious with links, verify sender
Malware	Computer Systems	Downloads, Infected Files	Steal Data, Disrupt Systems	Varies	Varies	Use antivirus, keep software updated, be careful with downloads
Data Leakage	Data	Accidental Exposure, System Vulnerabilities	Expose Sensitive Data	Varies	Varies	Use encryption, access controls, monitor for suspicious activity
Man-in-the-Middle (MITM)	Communication between device and server	Unsecured Wi-Fi, compromised networks	Eavesdrop, intercept or modify data	Moderate to high	Difficult	Use VPNs, avoid public Wi-Fi, use HTTPS websites

Drive-by Downloads	Mobile device	Compromised websites, malicious links	Install malware without user knowledge	Low	Difficult	Block pop-ups, avoid suspicious websites, keep software updated
Unsecured Wi-Fi Networks	Data transmitted over network	Public Wi-Fi hotspots	Intercept data, eavesdrop on communication	Low	Moderate	Use VPNs, avoid sensitive activities on public Wi-Fi
Clickjacking	Mobile user actions	Booby-trapped content, hidden buttons	Trick user into malicious actions	Varies	Difficult	Be cautious with online content, avoid suspicious websites, use security software.

V. RECOMMENDED BEST PRACTICES FOR MOBILE PHONES SECURITY

Individuals, organizations, and small businesses should consider the importance of being aware of Mobile security threats and the measures to counter them in the field of Mobile applications. According to literature studies related to Mobile security, the most related studies reported using built-in methods to reduce the negative effects of Malware and social engineering scams.

Mobile users in different society sectors and enterprises should understand the risks linked to physical and social factors. To enhance Mobile security, they should identify the range of issues related to both threats and best practices. Additionally, organizations should be aware of the factors that influence users' intentions and motivations to accept and use Mobile applications securely.

Finally, we recommend the mobile users, organizations and service providers to consider the following suggested best practices to protect their Mobile devices and Data and to ensure secure mobile transactions.

A. Be Aware of URLs you Visit during Internet Exploring

Refrain from clicking on links that seem to be spam or have unfamiliar URLs.

B. Use Strong and Different Password for Different Accounts

Avoid storing your passwords in your browser and make sure to use a unique password for each of your accounts.

C. Do Not Share Personal Information

You should avoid disclosing your sensitive information to strangers online. If you receive a call or message from someone claiming to be an official, make sure to verify their identity completely before sharing any details.

D. Be Cautious of Attractive Offers

Before accepting an offer as definite, pause and consider if it seems too good to be true. You can quickly find out whether it's a legitimate offer or a scam by researching the topic on Google.

E. Strengthen User Authentication

Prioritize user authentication by applying strong security measures on mobile devices. This involves using screen locks and activating authentication options like passwords, biometrics (such as fingerprint or facial recognition), or personal identification numbers (PINs). Focusing on user authentication helps improve device security and safeguard user data efficiently.

F. Install Anti-Virus Software

These programs can protect you from viruses and cyber-attacks.

G. Avoid Public Wi-Fi and the Use of virtual private network (VPN)

Using free public Wi-Fi networks on your mobile devices can be tempting. However, despite appearing safe, it actually raises the risk of malware infections and hackers gaining access to your smartphone data. When you connect to an unsecured public network shared by many users, using VPN becomes essential because it enhances online security and protects the privacy of your data while browsing the internet. With a VPN active, all your information is securely encrypted, ensuring that data transmitted from your mobile devices remains safe.

H. Regularly Update Mobile OSs and Apps to fix security flaws and vulnerabilities

It is important to consistently update your mobile operating system (like Android or iOS) and all installed apps. Doing so is vital because it allows users to receive the newest security patches and fixes from Google and Apple.

These updates tackle recent vulnerabilities and threats, while also adding performance and security enhancements. Keeping your OS and apps up to date greatly improves the security of your mobile devices.

I. Cloud Backups

Regularly backing up user data is a crucial method to avoid data loss or accidental deletion. It is essential to update the backup schedule as the volume of data grows over time. User data can include individual files (such as documents and spreadsheets), media files (like photos and videos), contacts, and other sensitive information. Cloud backup allows your data to be accessible from anywhere, making it easy to quickly restore all your information to a new device if your current one is damaged, lost, or replaced. Here is a guide on how to back up your data on iOS and Android devices:

- In iOS Mobile, select the iCloud option from Setting menu, then select Backup option from iCloud menu, after that make the iCloud Backup option ON.
- In Android mobile, select the Cloud Service from Setting menu, then select the Cloud Backup option from Cloud Service menu, after that set the Auto Backup option to be ON.

J. Organizations Security Approaches

In addition to above mobile security best practices, a set of security approaches that should be considered by different organizations were suggested in this work such as:

- Security Risk Management approach: should be continuously considered to prevent risks. This involves regularly reviewing and updating security strategies to address emerging challenges in mobile commerce.
- Threats Identification approach: involves managing mobile security risks and recognizing the different types of organizational threats. This is achieved by understanding unauthorized transactions, harmful malware attacks, and risks from third-party networks.
- Employee education: training the employee how to be aware of risks associated with mobile devices especially how to recognize phishing attempts; avoiding important transactions via public Wi-Fi; and routinely backing up data to recover from possible breaches.
- Good authentication techniques: used to protect access to different types of computing devices such as the implementation of two-factor authentication.
- Compliance and auditing approach: by maintaining a high level of security and ensuring that employee and other service providers adhere to security best practices by avoiding important transactions on public Wi-Fi, and routinely backup data to recover from possible breaches.
- Preventive measures approach: encompasses both physical and digital security measures that service providers should implement to effectively safeguard consumer information.

VI. CONCLUSION

Mobile attacks are increasing in volume and severity that expose users to various security threats. Common threats to mobile security include the theft of personal information, tracking of users, and malicious activities caused by limited device resources.

The paper addressed the critical needs and the importance of best practices that are recommended for mobile security for both individuals and organizations.

The paper highlighted the mobile risks, attacks and vulnerability from phishing to malware attacks. We described in details these attacks and threats and their different types. The paper outlined the best practices that are recommended to emphasize awareness and minimize risks for individuals and organizations.

Best practices for prevention mobile attacks and vulnerability were suggested to security awareness for both individuals and organizations.

• Security Software: Use antivirus and anti-malware tools to identify and reduce threats.
• Strong Authentication: Apply multi-factor authentication to protect against unauthorized access.
• User Education: Educate users about phishing techniques and safe browsing habits to lower the risk of attacks.

Finally, this work addressed many security approaches that should be conducted by organizations in different sectors. These approaches are: Security risk management approach; Threats identification approach; Compliance and auditing approach; and Preventive measures approach.

ACKNOWLEDGEMENT

The author would like to thank Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) for supporting Scientific researches.

REFERENCES

[1]. P. Weichbroth and L. Lysik, Mobile Security: Threats and Best Practices, Hindawi, Mobile Information Systems, Vol 2020, Article ID 8828078, pp:1-15, December 2020, https://doi.org/10.1155/2020/8828078

[2]. Georgina Gilmore and P. Beardmore, Mobile Security & BYOD for Dummies, Kaspersky lab limited edition, John Wiley & Sons Ltd, The Atrium Southern Gate Chichester, West Sussex, PO198SQ, England, 2013.

[3]. PMD Nagarjun and Shaik Ahamad, Review of Mobile Security Problems and Defensive Methods, International Journal of Applied Engineering Research, Vol.13, No.12, pp. 10256-10259, 2018, Research India Publications, ISSN 0973-4562, http://www.ripublication.com

[4]. Kevin Curran, V. Maynes and D. Harkin, Mobile device security, International Journal of Information and Computer Security, Vol. 7, No. 1, 2015.

[5]. OWASP, Mobile Top 10-2024: Final Release Updates, 2024, https://owasp.org/www-project-mobile-top-10/

[6]. Mohamed Ibrahim, G. Supayah, J. Bin Ibrahim, Mobile Security and Privacy In Smartphone Technology, International Journal of Computer Science and Information Technology Research, Vol.3, Issue.4, pp:345-350, December 2015, ISSN 2348-120X (online), www.researchpublish.com, Research Publish Journals

[7]. Sriram Vamsi Ilapakurthy, Bolstering the Mobile Cloud: Addressing Emerging Threats and Strengthening Multi-Layered Defenses for Robust Mobile Security, 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, pp:1-7, 23-25 October 2023, DOI: 10.1109/IOTSMS59855.2023.10325824

[8]. Marc Schmitt, Mobile Security for the modern CEO: Attacks, Mitigations, and Future Trends, 17 Jul 2022, arXiv.org , Vol. abs/2207.08105, DOI: 10.48550/arXiv.2207.08105

[9]. Mona Adlakha, Mobile Commerce Security and Its Prevention, Book Chapter, pp:141-157, Book: Securing Transactions and Payment Systems for M-Commerce, University of Delhi, IGI Global, 01 Jan 2016, ISBN13: 9781522502364|ISBN10: 152250236X|EISBN13: 9781522502371, DOI: 10.4018/978-1-5225-0236-4.ch007.

[10]. Andi Fitriah A., Arash H. Lashkari, and Mahdi D. Firoozjaei, Understanding Cybersecurity on Smartphones, Challenges, Strategies, and Trends, chapter: Mobile Application Security, pp 89-101, Springer International Publishing, 1st Jan 2024.

[11]. Won H. Park, et. al, A Study on Trend and Detection Technology for Cyber Threats in Mobile Environment, International Conference on IT Convergence and Security (ICITCS), IEEE Xplore, Macao, China, pp:1-40, 16-18 December 2013, DOI: 10.1109/ICITCS.2013.6717792

[12]. Teodor Mitrea and Monica Borda, Mobile Security Threats: A Survey On Protection and Mitigation Strategies, International Conference Knowledge-Based Organization, Sciendo, Vol. 26, Issue: 3, Pp:131-135, 3 Jun 2020.

[13]. Timothy Speed, et al, Mobile Security: How to Secure, Privatize, and Recover Your Devices, Packt Publishing, Limited, 10 Sep 2013, ISBN: 1849693609, 9781849693608

[14]. Nicholas Penning, at. al, Mobile Malware Security Challenges and cloud-based detection, 2014 International Conference on Collaboration Technologies and Systems (CTS), IEEE, 19-23 May 2014, pp:181-188, Minneapolis, MN, USA, IEEE Xplore: 31 July 2014, DOI: 10.1109/CTS.2014.6867562

[15]. Vaishnavi Bhavsar, A. Kadlak and S. Sharma, Study on Phishing Attacks, International Journal of Computer Applications (0975 – 8887) Vol.182, No. 33, December 2018.

[16]. Muhammad Nadeem, et al. Phishing Attack, Its Detections and Prevention Techniques, International Journal of Wireless Security and Networks, Vol.1, Issue.2, 2023 July–December, DOI: 10.37591/IJWSN

[17]. Liu Chengcheng, et. al, Directional fishing attack event discovery method and device, 12 may 2020.

[18]. Andrushchak I.Ye., Features of the Main Directions, Techniques and Methods of Protection Against Fishing At-Tacks, Computer-Integrated Technologies: Education, Science, Production, No. 47, pp:5-9, 2022, Doi: Https://Doi.Org/10.36910/6775-2524-0560-2022-47-01

[19]. Ma Zhuobu, and Guan Hainan, Method and device used for preventing fishing attack, 26 Feb 2014

[20]. Guo Zewen, Liming Wang, Yi Chen, Fei Zuo, Tao Li, Xiaomeng Zhou, Method and system for protecting account, preventing order from being tampered and preventing fishing attack based on graphical two-dimensional code, 11 Jul 2012

[21]. Kang Xin-zhen, Application of Trusted Computing Technology in Anti-fishing, Computer Engineering , 01 Jan 2008

[22]. Matthew Kosinski, What is smishing (SMS phishing), IBM, 10 Jun 2024, [Online]. Https://www.ibm.com/topics/smishing.

[23]. Eynan Lichterman, 6 Steps to Prevent Smishing Attacks, cybeready, The Human Readiness Company, August 27, 2024, https://cybeready.com/the-complete-guide-to-smishing/steps-to-prevent-smishing-attacks

[24]. Kenneth C. Laudon and Carol G. Traver, E-commerce, Business, Technology, Society, Global Edition, 16th edition. Pearson, 2020.

[25]. T.V. Mini, Jomy John, P.D. Siji, Unmasking Deception: Artificial Neural Networks in Smishing Detection for Cyber Security Fortification, International Journal of Electronics and Communication Engineering, Vol.11, Issue.7, 2024, SSRG, DIO: 10.14445/23488549/IJECE-V11I7P114

[26]. Ameen R. Mahmood and Sarab M. Hameed, Review of Smishing Detection Via Machine Learning, Iraqi journal of science , Vol 64 No 8 (2023), 30 Aug 2023, DOI: https://doi.org/10.24996/ijs.2023.64.8.42

[27]. Guillaume Gallet, Guillaume Guérard, Sonia Djebali, Automatic Smishing Detection System with Feedback Loops, International Journal of Data Science and Analytics, Research Square, 12 Aug 2024, doi: 10.21203/rs.3.rs-4760693/v1

[28]. Atif M. Memon, Ali Anwar, Colluding Apps: Tomorrow's Mobile Malware Threat, Vol.13, Issue.6, pp: 77 –81, 08 December 2015, Print ISSN: 1540-7993, E-ISSN: 1558-4046, DOI: 10.1109/MSP.2015.143

[29]. Yean Li Ho and Swee-Huay Heng, Mobile and ubiquitous malware, MoMM '09: Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, ACM, pp:559 – 563, 14 Dec 2009, https://doi.org/10.1145/1821748.1821856

[30]. Abhijit Bose and K.G. Shin, On Mobile Viruses Exploiting Messaging and Bluetooth Services, 2006 Securecomm and Workshops, pp 1-10, 28 August 2006 - 01 September 2006, Baltimore, MD, USA, IEEE Xplore: 15 May 2007, ISBN:1-4244-0422-3, DOI: 10.1109/SECCOMW.2006.359562

[31]. Alberto Berretti and Simone Ciccarone, A Monte Carlo method for the spread of mobile malware, . arXiv: Social and Information Networks, 03 Dec 2015

[32]. Hsiu-Sen Chiang, and Woei-Jiunn Tsaur, Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology, 2010 IEEE Second International Conference on Social Computing, Minneapolis, pp:1080-1085, MN, USA, 20-22 August 2010, IEEE Xplore: 30 September 2010, DOI: 10.1109/SocialCom.2010.160

[33]. Teodor MITREA and Monica BORDA, Mobile Security Threats: A Survey on Protection and Mitigation Strategies, International conference KNOWLEDGE-BASED ORGANIZATION 26(3):131-135, June 2020, DOI: 10.2478/kbo-2020-0127

[34]. Attia Qamar, Ahmad Karima, and Victor Chang, Mobile malware attacks: Review, taxonomy & future directions, Future Generation Computer Systems, Vol. 97, No.5, March 2019, DOI: 10.1016/j.future.2019.03.007

[35]. Android Trojan Horse Spyware Attack: A Practical Implementation, 2024 12th International Symposium on Digital Forensics and Security (ISDFS), 29-30 April 2024, San Antonio, TX, USA, IEEE Xplore: 15 May 2024, ISSN: 2768-1831, ISSN: 2837-827X, DOI: 10.1109/ISDFS60797.2024.10527296

[36]. Akhil S, Neeraja M Nair and Arun R, Detection and Prevention of Keylogger Spyware Attacks, International Journal of Computer Engineering and Technology, Vol.5, Issue.12, pp. 167-172, December 2014, ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online).

[37]. Sidhant Chourasiya, et al, Pegasus Spyware: A Vulnerable Behaviour-based Attack System, 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India , 19-21 July 2023, Date Added to IEEE Xplore: 16 August 2023, DOI: 10.1109/ICECAA58104.2023.10212163

[38]. Ajith Peter Vianney R., S. Manikandan, A. C. Santha Sheela, Efficient Password Mechanism to Overcome Spyware Attack: Quantum Network and AI, Book Chapter5, pp:61-74: Multidisciplinary Applications of AI and Quantum Networking, Advances in computational intelligence and robotics book series, DOI: 10.4018/979-8-3693-9336-9.ch005

[39]. C. Shoba Bindu, Click based Graphical CAPTCHA to thwart spyware attack, 2015 IEEE International Advance Computing Conference (IACC), 12-13 June 2015, Banglore, India, Date Added to IEEE Xplore: 13 July 2015, DOI: 10.1109/IADCC.2015.7154723

[40]. Aadil Khan and Ishu Sharma, SAndro: Artificial Intelligence Enabled Detection Framework of Adware Attacks on Android Machines, 2023 Global Conference on Information Technologies and Communications (GCITC), 01-03 December 2023, Bangalore, India, IEEE Xplore: 18 April 2024, DOI: 10.1109/GCITC60406.2023.10426218

[41]. Tommy Blizard and Nikola Livic, Click-fraud monetizing malware: A survey and case study, 2012 7th International Conference on Malicious and Unwanted Software, 16-18 October 2012, Fajardo, PR, USA, IEEE Xplore: 14 February 2013, DOI: 10.1109/MALWARE.2012.6461010

[42]. Reem A. Alzahrani and Malak Aljabri, AI-Based Techniques for Ad Click Fraud Detection and Prevention: Review and Research Directions, Journal of Sensor and Actuator Networks, Vol.12, No.1, 4 December 2022, DOI: 10.3390/jsan12010004

[43]. Paulo S. Almeida and Joao Gondim, Click Fraud Detection and Prevention System for Ad Networks, Journal of Information Security and Cryptography (Enigma), 5(1):27 January 2019, DOI: 10.17648/jisc.v5i1.71

[44]. Hao Wen, Hongming Wang, Jiaxuan Liu, Yuanchun Li, DroidBot-GPT: GPT-powered UI Automation for Android, arXiv.org 14 April 2023, DOI:10.48550/arXiv.2304.07061, Corpus ID: 258170084

[45]. Kavya A P, Manoj B R, Monish L, Manohara H , Android Operated Mobile Robot for Agriculture Purpose, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 10 Issue:6, pp 3142-3145, June 2022, ISSN: 2321-9653.

[46]. Abubakar Umar, et al, Development of an Android Based Voice Controlled Autonomous Robotic Vehicle, Engineering Proceeding, Engineering Proceeding, 15 November 2023, Eng. Proc. 2023, 56, x. https://doi.org/10.3390/xxxxx

[47]. Laura García; Ricardo J. Rodríguez, A Peek under the Hood of iOS Malware, 2016 11th International Conference on Availability, Reliability and Security (ARES), 31 August 2016 - 02 September 2016, Salzburg, Austria, IEEE Xplore: 15 December 2016, DOI: 10.1109/ARES.2016.15

[48]. Madihah Mohd Saudi,, et al, iOS mobile malware analysis: a state-of-the-art, Journal of Computer Virology and Hacking Techniques, Vol.20, pages 533–562, 18 May 2023

[49]. Olav Lysne, Development of ICT Systems, The Huawei and Snowden Questions, Simula SpringerBriefs on Computing ((SBRIEFSC, volume 4)), book chapter, First Online: 20 February 2018, pp 31–38.

[50]. Thomas S. Hyslip and George W. Burruss, Ransomware, Book Chapter in Handbook on Crime and Technology, 28 Mar 2023, pp:86–104, DOI: https://doi.org/10.4337/9781800886643.00013

[51]. Yap Jia Seng, et, al, In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations, Computer Science and Mathematics, 02 Sep 2024 PrePrints.org, DOI:10.20944/preprints202408.2261.v1

[52]. Ezekiel Ologunde, Ransomware, 15 May 2024, SSRN: https://ssrn.com/abstract= 4823359 or http://dx.doi.org/10.2139/ssrn.4823359

[53]. Madihah Mohd Saudi, Tamara Nusairat, Azuan Ahmad, Muji Setiyo, Enhancing Cybersecurity: Ransomware Detection - A Proof of Concept Study, Journal of Advanced Research in Applied Sciences and Engineering Technology, 04 Oct 2024 , DOI: https://doi.org/10.37934/araset.54.2.252268

[54]. Ömer Söner, Gizem Kayisoglu, Pelin Bolat, Kimberly Tam, An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors, Proceedings Of The Institution of Mechanical Engineers, Part O: Journal of Risk And Reliability, 01 Oct 2024

[55]. Avijit Mallik, MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS, Jurnal Pendidikan Teknologi Informasi, Vol.2, No.2, October 2018, pp:109 - 134

[56]. Mohammed Muniru Iddrisu, et al, An improved man-in-the-middle (MITM) attack detections using convolutional neural networks, Multidisciplinary Science Journal , Vol. 7 Issue 3 (2025), e2025129, 16th September 2024, DOI: 10.31893/multiscience.2025129

[57]. K. Venkateswara Rao; B. Renu Akshaya; G. Gershon Satvik; B. Rohith; G. Chakrika Bala Lahari, Machine Learning based Man-in-the-Middle Attack Prediction, 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 05-07 June 2024, Salem, India, Date Added to IEEE Xplore: 02 July 2024, DOI: 10.1109/ICAAIC60222.2024.10575798

[58]. Gwamaka Henry Mwakajwanga, Othmar Othmar Mwambe, Digital-Signature Oriented Steganography Approach against Man-in-the-Middle Attack, International journal of interactive mobile technologies, vol.18, No. 16, pp:158-173, 27 Aug 2024

[59]. Manesh Thankappan, Helena Rifà-Pous, Carles Garrigues, A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks, International Journal of Information Security , Vol.23, No.6, pp:3527-3546, 14 Aug 2024, DOI: 10.1007/s10207-024-00899-9

[60]. Aryaman, Nenavath Srinivas Naik, Satyanarayana Vollala, Ruhul Amin , Detecting and predicting countermeasures against clickjacking, Vol.6, Issue.5, 06 February 2023, https://doi.org/10.1002/spy2.302

[61]. D.Kavitha and S.Ravikumar, Click jacking Vulnerability Analysis and Providing Security against WEB Attacks Using White listing URL analyzer, International Journal of Computer Techniques – Vol. 2, Issue.3, pp:61-67, May-June 2015, ISSN: 2394-2231 http://www.ijctjournal.org

[62]. Yashodha Patil, Detection of Clickjacking Attacks using the Extreme Learning Machine algorithm, MSc Cyber Security, School of Computing, National College of Ireland 01 Jan 2020, Corpus ID: 237125481

[63]. Chao Feng, et al., Systemic Implications of CVE-2023-33246 A Closer Look at Remote Code Exploitation Mechanisms, 2024 15th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 13-15 August 2024, IEEE Xplore: 22 August 2024, DOI: 10.1109/ICICS63486.2024.10638289

[64]. Tong Liu, Zizhuang Deng, Guozhu Meng, Yuekang Li, Kai Chen, Demystifying RCE Vulnerabilities in LLM-Integrated Apps, CCS '24: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, pp: 1716 – 1730, 6th Sep 2023, https://doi.org/10.1145/3658644.3690338

[65]. Feng Xiao, et al., Understanding and Mitigating Remote Code Execution Vulnerabilities in Cross-platform Ecosystem, CCS '22: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp: 2975 – 2988, 07 November 2022 , https://doi.org/10.1145/3548606.3559340

[66]. Enbo Sun, Jiaxuan Han, Yiquan Li, Cheng Huang, A Packet Content-Oriented Remote Code Execution Attack Payload Detection Model, Future Internet 2024, 16(7), 235; 2 July 2024, https://doi.org/10.3390/fi16070235

[67]. Wenqi Wei, et. al, Data Poisoning and Leakage Analysis in Federated Learning, pp 73–108, 04 September 2024, chapter in Handbook of Trustworthy Federated Learning , Springer optimization and its applications

[68]. Jie Wang, et. al, Data Leakage Behavior Recognition Based on Cyclical Learning Rate based Long-Short Term Memory, 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), 23-24 February 2024, Raichur, India, IEEE Xplore: 18 April 2024, DOI: 10.1109/ICICACS60521.2024.10498905

[69]. Mohamed A. Bouke, Saleh A. Zaid, Azizol Abdullah, Implications of Data Leakage in Machine Learning Preprocessing: A Multi-Domain Investigation, The Journal of Supercomputing, 12 Jul 2024, doi: 10.21203/rs.3.rs-4579465/v1

[70]. Svetlana Syarova, et. al, Data Leakage Prevention and Detection in Digital Configurations: A Survey, Environment. Technology. Resources. Rezekne, Latvia, Proceedings of the 15th International Scientific and Practical Conference, Vol.2 , 22 Jun 2024, pp:253-258, Rezekne, Latvia , DOI: https://doi.org/10.17770/etr2024vol2.8045

[71]. Sultan Alneyadi, E. Sithirasenan, V. Muthukkumarasamy, A survey on data leakage prevention systems, Journal of Network and Computer Applications, Vol.62, Feb 2016, pp:137-152, https://doi.org/10.1016/j.jnca.2016.01.008Get rights and content

[72]. Periasamy J K, Cindy Catherine A, Elamathi R, Subhiksha S, Data Leakage Vulnerability Assessment, 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), Chennai, India, 14-15 December 2023, IEEE Xplore: 19 March 2024, DOI: 10.1109/ICCEBS58601.2023.10448949

[73]. Julia Narvaez, et. al, Barbara Endicott-Popovsky, Drive-by-downloads, 2010 43rd Hawaii International Conference on System Sciences (HICSS), 05-08 January 2010, IEEE Xplore: 11 March 2010, Honolulu, HI, USA, ISSN: 1530-1605, DOI: 10.1109/HICSS.2010.160

[74]. Nissy Sombatruang, M. Angela Sasse, and Michelle Baddeley, Why do people use unsecure public Wi-Fi? An investigation of behaviour and factors driving decisions, *STAST '16*, December 05-05, 2016, Los Angeles, CA, USA , ACM ISBN 978-1-4503-4826-3/16/12. http://dx.doi.org/10.1145/3046055.3046058

[75]. Hamza Azam, et. al, Wireless Technology Security and Privacy: A Comprehensive Study, 9 November 2023, https://www.preprints.org/manuscript/202311.0664/v1, doi: 10.20944/preprints202311.0664.v1

[76]. Wade, Unsecured WiFi network | What are the risks of using WiFi hotspots?, TheBestVPN.UK, Doanloaded Date: 4th October2025, https://thebestvpn.uk/unsecured-wifi-network/#:~:text=And%20this%20technique%20allows%20hackers,and%20access%20all%20your%20data.

[77]. Yong Wang and Yazan Alshboul, Mobile security testing approaches and challenges, 2015 First Conference on Mobile and Secure Services (MOBISECSERV), 20-21 February 2015, Gainesville, FL, USA, IEEE Xplore: 02 April 2015, Electronic ISBN:978-1-4799-7428-3, DOI: 10.1109/MOBISECSERV.2015.7072880

[78]. Timothy Speed , et. al, Mobile Security: How to Secure, Privatize, and Recover Your Devices September 2013, Packt Publishing, ISBN:978-1-84969-360-8, 10 September 2013.

[79]. Paul Ruggiero and Jon Foote, Cyber Threats to Mobile Phones, U.S Department of Security Homeland, Carnegie Mellon University, US-CERT, 2011.

