# Cybersecurity Concerns on Mobile Phones: A Systematic Review

**Noluntu Mpekoa**
University of Johannesburg, South Africa

noluntum@uj.ac.za

**Abstract:** Mobile devices have become an important part of our everyday lives since they offer access to a large variety of ubiquitous services. Because of this technological revolution, the deployment of mobile systems can offer sophisticated and complex services; like mobile payments, mobile health and even mobile government. Due to these astounding reasons, the number and types of vulnerabilities exploiting these services and communication channels have increased as well. This signifies that continuous investigation and understanding of the challenges and issues in mobile platforms is crucial. Hence, the primary aim of this study was to conduct a systematic literature review on mobile phone attacks, to gain a better understanding of the different attacks and threats to mobile devices. The focus was on four critical elements of the device, which are the: mobile operating system, firmware, applications and websites and lastly, connectivity. The PRISMA 2020 statement guided the systematic literature review. 675 journal articles and conference papers published between 2018 and 2024 were retrieved and 32 were considered for this study. The findings suggest that in 2023 alone, the number of cyber-attacks on mobile devices surged to 33 million. Also, the study found that there are various malware that can attack mobile devices namely virus, worms, botnets, trojans, ransomware, backdoors and root kits, due to these attacks the users' privacy is compromised. These attacks exploit mobile security vulnerabilities to capture sensitive data or impersonate trusted entities. Cybercriminals recurrently dispersed mobile threats through both official and unofficial application stores. Malicious applications and websites are amongst the most popular attacks, followed by mobile ransomware and phishing. This study highlights various attacks that warrant further investigation, and future research should examine the controls and safeguards associated with each security issue. Additionally, there is a pressing need to advance lightweight, real-time malware detection systems that can operate effectively on mobile devices with limited resource.

**Keywords:** Mobile security, Mobile attacks, Mobile firmware attacks,Mobile ransomware, Mobile threats

## 1. Introduction

Mobile devices are indispensable in this digital age, providing immediate access to a vast array of essential services. Citizens carry their mobile phones with them everywhere, making public services accessible at any time and in any place. With just a few taps, citizens can shop online, connect on social media, and handle banking transactions right from their phones (Alotaibi *et al.*, 2024). This widespread access has revolutionised citizen interaction with services, placing unparalleled convenience directly at their fingertips. The technological revolution brought about by mobile systems provides a range of advanced and intricate services, including mobile television, mobile payments, and mobile health. Mobile devices hold a wealth of personal and professional information, making it crucial to protect them from unauthorized access (Bubukayr & Almaiah, 2021). Mobile phone security involves a range of policies, programs, and activities designed to protect the user's privacy and ensure the integrity of the device. The increasing popularity of mobile devices has led to a rise in cybercriminals who are taking advantage of this trend by engaging in various scams (Alure & Puri, 2021). As mobile devices and applications handle more data, the chances of discovering potential threats and attacks also increase. The number and variety of vulnerabilities targeting these services and communication channels have risen significantly. Malware developers create and spread harmful applications designed to steal sensitive information and credentials. Their goal is also to immobilize mobile devices (Bhavan *et al.*, 2024).

Thus far, few systematic reviews on mobile phone security have been executed. This includes reviews that address challenges related to mobile phone security and privacy, as well as those that focus on mobile phone attacks. The current research landscape reveals a significant gap in studies examining mobile phone operating systems, firmware, applications, and websites, especially regarding connectivity issues (Diallo, Samhi, Bissyandé, & Klein, 2024). As such, there is a need for a deeper understanding of the mobile phone security that considers its various aspects (Zhang, Wang, He & Liu, 2020). This study's literature review aims to build upon previous research by identifying key security issues related to mobile phones. It introduces a classification scheme that takes a holistic approach to mobile phone security. The review categorises security issues based on various domains, including mobile phone operating systems, firmware, applications and websites, and connectivity, while excluding considerations related to the physical device itself. This assessment aims to identify the gaps, challenges, and future work needed in mobile phone security. To achieve this goal, the study adheres to the guidelines set forth by Page *et al.* (2021) in their Preferred Reporting Items for Systematic Reviews (PRISMA). The research offers an overview of the current state of mobile phone security, highlighting key insights for future studies. It emphasises a comprehensive, multi-faceted approach to the topic.

This research asserts the necessity of developing and implementing effective security measures to address the potential threats to sensitive data arising from the use of mobile devices. It is imperative to engage in ongoing investigation and thoroughly understand the challenges and issues surrounding mobile platforms, this is key to driving success and innovation in the field. The remainder of the paper is as follows: Section 2 gives background and current state of mobile phone security, by identifying and classifying mobile phone security issues. Section 3 provides a detailed methodology used to conduct the study. Section 4 offers findings, discussions, and future work. While Section 5 concludes the paper.

## 2. Mobile Device Domains and Research Gap

Mobile phones, commonly referred to as cellular phones, are compact, affordable, and portable devices designed for communication. Mobile phones boast a broader array of features and capabilities, making them more versatile and powerful in today's digital landscape. This technological evolution has transformed how we interact with mobile devices, leading to their widespread use (Xu *et al*., 2019). Mobile devices can be categorised into eight main types: Notebooks, Tablets, Mobile Media Players, Mobile Gaming Devices, Mobile Phones, Smartphones, Personal Digital Assistants (PDAs), and Industrial Mobile Devices (Meng *et al.*, 2018). This study aims to explore these categories in detail, emphasising the various attacks and threats that target these devices. By examining these elements, a better understanding can be gained of the security challenges associated with mobile devices. The focus was on four critical elements of mobile phones, which are the: mobile operating system, firmware, applications and websites, and lastly, connectivity.

### 2.1 Mobile Device Domains

Over the past decade, mobile devices have evolved significantly, transforming into powerful data repositories capable of storing vast amounts of both personal and organisational information. The increasing use of smartphones and tablets has made them an integral part of daily life for many individuals, seamlessly blending into routines and enhancing user's ability to manage information on the go (Zhu *et al.*, 2018). Common examples of mobile phone usage include activities such as sending emails, transferring money through mobile banking, making calls, texting, browsing the Internet, viewing documents, storing personal and confidential information, shopping online, and playing games (Meng *et al.*, 2018). Many of these applications handle sensitive data, making the risks significant if there is a loss of information due to privacy breaches. Protecting this data is crucial to avoid potential consequences (Tang *et al.*, 2020).

As the number of vulnerabilities and threats continues to grow, it is essential to implement security measures that specifically target the different areas of mobile devices. This study introduces a comprehensive classification scheme for mobile phone security issues, emphasising a holistic approach. Mobile phone security concerns were identified and categorised according to various domains, including mobile operating systems, firmware, applications and websites, and connectivity. Notably, this classification excludes considerations related to physical device security. This section explores the various domains related to mobile phone security.

- **Mobile phone operating systems:** enable smartphones, tablets, and other devices to run applications and programs. They act as an interface between the device's hardware and its software functions. Some common examples of mobile operating systems include Android, iOS, Windows Phone, Symbian, BlackBerry OS, and webOS (Nawshin *et al.*, 2024).
- **Mobile firmware:** is a program embedded in hardware devices to ensure they operate effectively. Devices such as cameras, mobile phones, network cards, printers, scanners, and television remotes all rely on firmware stored in their memory. This firmware enables the hardware to function smoothly and work seamlessly with different software applications (Alure & Puri, 2021).
- **Mobile applications and websites:** are software programs designed to run on smartphones, tablets, and smartwatches. These apps are convenient for use on the go and differ from desktop applications, which are meant for traditional computers. In contrast, web applications operate through mobile web browsers rather than being installed directly on the device (Alotaibi *et al.*, 2024; Debnath & Jain, 2024).
- **Mobile connectivity:** Mobile connectivity refers to the ability of devices to connect to networks and communicate with one another. It encompasses various means of connections, such as cellular networks (e.g., 5G), Wi-Fi, Bluetooth, and satellite networks. These technologies enable mobile users to access the internet and share data without being restricted to a specific location or device (Sharma *et al.*, 2024).

The definitions in this section helped classify the relevant literature and discussions in these areas. This understanding can guide other researchers in creating tailored solutions for each domain and addressing existing gaps.

### 2.2 Mobile Security Challenges and Research Gaps

This section explores the current security challenges that mobile devices encounter and highlights gaps in research through a review of relevant literature. Mobile application security has become a critical concern in developing countries, as highlighted by Diallo, Samhi, Bissyandé, and Klein (2024). The study explores the current state of research on mobile application security, particularly in developing countries. To achieve this, the authors conducted a systematic literature review to analyse the research directions taken by previous studies, the various security concerns addressed, and the techniques employed by researchers to highlight or mitigate application security issues. Their findings support the initial assertion that there is a scarcity of literature specifically focusing on mobile application security in the context of developing countries. Among the various security concerns identified, vulnerability detection emerged as the predominant research topic. Additionally, the review revealed that FinTech applications are frequently highlighted as the primary focus within the relevant literature.

Bubukayr and Almaiah (2021) highlight that mobile phone users are increasingly taking on sensitive and critical tasks, which makes these devices particularly attractive targets for attackers. They express concern over the security vulnerabilities inherent in mobile devices and their applications. Their study includes a comprehensive literature review, examining a range of selected studies that focus on major cybersecurity threats impacting smartphones and applications. Key threats identified include malware attacks, phishing attacks, software failures, Denial of Service (DoS) attacks, as well as sniffing and spoofing attacks, and physical attacks. The authors reviewed twenty previous studies, pinpointing significant cybersecurity threats that could compromise mobile systems. They categorised these threats according to four critical assets of a smartphone: the device itself, the data it contains, the applications it runs, and network connectivity. Additionally, they prioritised the most significant threats, shedding light on the critical challenges facing mobile security today.

Keteku *et al.* (2024) highlight that the rising popularity of mobile applications has led to a significant increase in the number of new apps entering the market. This surge has attracted the attention of security professionals and researchers due to the recent emergence of various types of mobile malware. The authors emphasise that as the mobile phone industry continues to grow, the likelihood of these devices being exploited for criminal activities is expected to rise further in the future. Their study reviews existing literature on malware detection and prevention specifically for Android mobile devices, analysing major studies and topics in the field. They reference various sources, including articles, journals, and digital resources such as internet security publications and scientific conferences. Their findings indicate that there are increasingly more instances of malicious software being reported each year. To combat this threat, antivirus companies, retail markets, and computer programmers are continuously working to enhance malware detection methods through cryptographic techniques. The study concludes with a recommendation to utilise cryptographic technologies to prevent mobile phone malware.

This research argues for the necessity of a deeper understanding of the mobile phone phenomenon, particularly regarding the multifaceted aspects of mobile phone security. The literature review of this study aims to build upon previous work in this field by systematically identifying and categorising mobile phone security issues. To do so, it employs a holistic approach that classifies these issues according to different mobile phone domains, including operating systems, firmware, applications, websites, and connectivity. This comprehensive classification scheme not only highlights the various security challenges but also emphasises the interconnected nature of mobile phone security.

### 2.3 Contribution

The primary contribution of this paper is twofold. First, it provides a comprehensive overview of current studies that can assist researchers in pinpointing research gaps in mobile phone security. Second, it highlights specific mobile phone domains that may aid researchers in designing targeted security tools and systems. In conclusion, this study offers suggestions for future research opportunities within these domains, encouraging further exploration to enhance the overall state of mobile phone security.

## 3. Research Methodology

The primary aim of this study was to conduct a systematic literature review on mobile phone attacks to enhance our understanding of the various threats and vulnerabilities targeting mobile devices. This review focused on four critical elements: the mobile operating system, firmware, applications and websites, and connectivity, while intentionally excluding the physical aspects of the device. By examining these key areas, the study seeks to illuminate the diverse landscape of mobile device security threats. A systematic literature review provides a comprehensive and detailed understanding of a specific topic, facilitating deep insights into the subject matter (Kralik, Visentin & Van Loon, 2006). Known for their methodological rigor, systematic reviews can be applied across various research domains and areas, enhancing their versatility and usefulness in academic inquiry. The systematic literature review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement. Initially published in 2009, the PRISMA statement was developed to assist systematic reviewers in transparently reporting the rationale, methodology, and findings of their reviews (Page *et al.*, 2021).

The main keywords used during the search were restricted to mobile phone threats, mobile phone attacks, mobile phone security, mobile app attacks, mobile device attacks, and mobile device threats. To capture as many relevant studies as possible, the study conducted electronic searches using Google Scholar and the Scopus database dating back to 2018 (Table 1 below). Articles and studies most relevant to the research theme were considered for this study. The query below was used on the Scopus database, which yielded 26 journal articles and conference papers from 2018-2024. Articles not focusing on mobile phone security and not written in English were excluded, all articles published before 2018 and not peer reviewed were also excluded.

> mobile phone threats AND mobile phone attacks AND mobile phone security AND mobile app attacks AND mobile device attacks AND mobile device threats

Then next was the Google Scholar database, the following query was also utilised, which yielded 649 journal articles and conference papers from 2018 to 2024.

> mobilephone threats* AND mobilephone attacks* AND mobilephone security* AND mobile app attacks* AND mobile device attacks* AND mobile device threats

**Table 1*:* Systematic Literature Review Approach**

| Database | Timespan | Keywords | 1st Round Results | Titles, abstracts, and conclusions | Research Aim |
|---|---|---|---|---|---|
| **Scopus** | 2018-2024 | mobile phone threats, mobile phone attacks, mobile phone security, mobile app attacks, mobile device attacks, and mobile device threats | 26 | 8 | 3 |
| **Google Scholar** | | | 649 | 116 | 29 |

A total of 675 journal articles and conference papers published between 2018 and 2024 were retrieved. Titles, abstracts, and conclusions of conference papers and documents were reviewed and 124 were considered. Then the authors reviewed the full-text articles for eligibility, excluding papers that did not contribute to the research aim (gaining a better understanding of the different attacks and threats to mobile devices, focusing on mobile operating system, firmware, applications and websites, and lastly, connectivity) were eliminated. In total, 32 papers were identified for qualitative analysis, as illustrated in Table 1 above. The following sections present the findings and discussion derived from this analysis.

## 4. Findings, Discussions and Future Research

Modern mobile devices offer substantial storage capacity and a diverse array of applications and connectivity options (Gimba & Ariffin, 2024). This review analysed 32 scholarly articles, highlighting several critical findings, including the identification of significant vulnerabilities within mobile operating systems and applications.

### 4.1 Findings and Discussions

The analysis of the findings, based on the proposed classification scheme for selected mobile domains, reveals noteworthy insights. The categories examined include: 1) mobile operating systems, 2) firmware, 3) applications

and websites, and 4) connectivity. Among the articles reviewed, 22% focused on issues related to mobile operating systems, and another 22% addressed mobile firmware concerns. In contrast, the majority of articles—45%—centered on mobile applications and websites, indicating that this is the most discussed area. Additionally, 25% of the articles explored issues related to mobile connectivity. As shown in Table 2 below, the prominence of discussions surrounding mobile applications and websites suggests that most authors are keen on identifying challenges within this domain. Consequently, the solutions developed will likely be concentrated in this area as well.

**Table 2: Aligning research aim with SLR sources**

| Author | Mobile Operating System | Firmware | Apps and Websites | Connectivity |
|---|---|---|---|---|
| Rupprecht *et al.* (2018) | | | | X |
| Nawshin *et al.* (2024) | X | | | |
| Gautam *et al.* (2023) | | | X | |
| Arunakumari, Shrivathsa & Vinodkumar (2022) | | | X | |
| Yao & Zimmer (2020) | | X | | |
| Xu, Diao, Li, Chen & Zhang (2019) | | | | X |
| Diallo, Samhi, Bissyandé & Klein (2024) | | | X | |
| Leguesse *et al.* (2021) | | | X | |
| Debnath & Jain (2024) | | | X | |
| Sun, Garcia, Salles-Loustau & Zonouz (2020) | | X | | |
| Alotaibi *et al.* (2024) | | | X | |
| Niveditha & Ananthan (2019) | X | | | |
| Sharma *et al.* (2024) | | | | X |
| Gimba, & Ariffin (2024) | | | X | |
| Zhang, Wang, He, & Liu (2020) | | | X | |
| Sharma, Johri, Goel & Gupta (2018) | | | X | |
| Sutter & Tellenbach (2023) | X | X | | |
| Meng *et al.* (2018) | | | | X |
| Alepis (2019) | X | | X | |
| Zhu *et al.* (2018) | | | X | |
| Dahiya *et al.* (2024) | | X | | X |
| Mehrnezhad, Toreini, Shahandashti & Hao (2018) | | | X | |
| Tang *et al.* (2020) | | | | X |
| Bhavan *et al.* (2024) | X | | | |
| Jing (2021) | X | | | |
| Doreswamy, Lokhande & Uttam (2021) | | | X | |
| Kalyani, Agarwal & Sharma (2020) | | | X | |
| Hou *et al.* (2022) | | X | | |
| Gunn *et al.* (2022) | X | | X | X |
| Alure & Puri (2021) | | X | | |
| Hou *et al.* (2023) | | X | | |
| Sousa & Reis (2024) | | | | X |
| Frequency | 22% | 22% | 47% | 25% |

In 2023, Kaspersky reported a significant rise in attacks targeting mobile devices, with nearly 33 million incidents recorded—an increase of 50% from the previous year. The primary threat to mobile devices was adware,

accounting for 40.8% of threats. Among the various types of malware, Trojans emerged as the most concerning, representing over 95% of mobile malware instances. Furthermore, it was observed that more than 98% of mobile banking attacks specifically targeted Android devices (Kaspersky, 2023).

### *4.1.1 Attacks and threats to mobile operating system domain*

Mobile devices face significant security challenges, primarily due to malware attacks that expose them to various threats. Several types of malware target these devices, including viruses, worms, ransomware, backdoors, and rootkits. Such attacks can severely compromise user privacy, as noted by Niveditha and Ananthan (2019). The most widely used mobile operating systems include Android, iOS, Windows Phone, and Linux (StatCounter, 2024), which are highlighted in Table 3. Notably, seven out of the 32 articles reviewed specifically addressed security issues related to mobile operating systems.

**Table 3: Authors worked on Mobile Operating Systems**

| Author | Mobile Operating Systems | | | | | | |
|---|---|---|---|---|---|---|---|
| | Android | Symbian | iOS | Windows | Blackberry | Linux | Other |
| Nawshin *et al.* (2024) | √ | | √ | | | | |
| Niveditha & Ananthan (2019) | √ | | | | | | |
| Sutter & Tellenbach (2023) | √ | | | | | | |
| Alepis (2019) | √ | | | | | | |
| Bhavan *et al.* (2024) | | | √ | | | | |
| Jing (2021) | √ | | | | | | |
| Gunn *et al.* (2022) | √ | √ | √ | √ | √ | √ | √ |
| Frequency | 85% | 14% | 43% | 14% | 14% | 14% | 14% |

A significant portion of the selected studies, specifically 85%, focused on the Android operating system. This focus aligns with StatCounter Global Stats (2024), which reports that Android holds 71.17% of the global market share. As an open-source platform, Android is particularly vulnerable to security threats due to its open environment, extensive user base, customization options, and often delayed security patches. In contrast, 43% of the studies examined the iOS operating system, which correlates with StatCounter Global Stats (204), indicating that iOS commands 28.33% of the market. iOS is generally regarded as more secure, as it restricts the installation of malicious applications and prevents unauthorized data access. This disparity in focus may explain why researchers are more inclined to study the Android operating system, given its susceptibility to a larger number of mobile device attacks.

Researchers such as Alepis (2019), Sutter & Tellenbach (2023), Bhavan *et al.* (2024), and others have proposed several techniques aimed at mitigating issues in mobile malware detection. These techniques include differential privacy, homomorphic encryption, and federated learning. Federated learning represents a contemporary approach that contrasts with traditional machine learning and deep learning methods used for detecting mobile malware. Recent studies, including those by Nawshin *et al.* (2024), have examined the risks associated with implementing federated learning in real-world applications. They recommend strategies to develop a secure federated learning framework specifically tailored to enhance the efficacy of mobile malware detection.

### *4.1.2 Attacks and threats to mobile firmware domain*

Mobile phone firmware security issues remain one of the least researched topics in cybersecurity, as highlighted in Table 2. Firmware attacks pose a significant and real threat to mobile devices (Yao & Zimmer, 2020). This is because firmware, which is the code controlling a device's hardware components, is typically the first code that runs when the device is powered on. A successful firmware attack can result in long-term access to the device, data loss, or unauthorised modifications to the system (Hou *et al.*, 2022). As noted by Sutter & Tellenbach (2023), detecting and mitigating malware and software vulnerabilities within mobile device firmware is a complex challenge that often requires specialised expertise in customising firmware formats. This complexity is further compounded by the fact that users have no say in the software pre-installed on their devices, leading to a significant lack of transparency and control. Unauthorised access to personal devices can severely compromise user privacy, enabling attackers to monitor online activities, steal sensitive information, or even gain remote control of the devices (Hou *et al.*, 2023; Alure & Puri, 2021). While some research has concentrated on the security of customised Android firmware (Hou *et al.*, 2022; Yao & Zimmer, 2020), other studies have focused on

developing efficient analysis tools or examining specific aspects of firmware security (Dahiya *et al.*, 2024; Sun, Garcia, Salles-Loustau & Zonouz, 2020). This indicates a need for a broader exploration of firmware security to mitigate these growing threats effectively.

#### *4.1.3 Attacks and threats to mobile applications and websites domain*

Mobile devices have evolved into powerful multi-purpose computing platforms that support a wide variety of applications (Gautam *et al.*, 2023). The ability to easily install third-party applications greatly enhances their basic functionality. These applications range from gaming and office tools to banking services, among others (Diallo, Samhi, Bissyandé & Klein, 2024). According to Arunakumari, Shrivathsa, and Vinodkumar (2022), millions of Android applications are downloaded daily, often from both trusted sources like the Google Play Store and untrusted ones. This widespread downloading practice has led to a significant number of mobile devices becoming infected with malicious applications (Zhang, Wang, He & Liu, 2020). Various authors have identified several types of attacks targeting mobile phone applications, including:

- **Malicious apps**: apps that may be installed on a device without the user's knowledge or downloaded from unauthorised app stores (Alepis, 2019; Zhu *et al.*, 2018).
- **Mobile malware**: malicious software that can steal personal information, alter device settings, or send phishing messages (Debnath & Jain, 2024).
- **Phishing attacks**: users are targeted while downloading or browsing an app. Once the app is installed, it can collect personal information and send it to the attacker (Debnath & Jain, 2024; Alepis, 2019).
- **Data leakage**: hostile applications that can transfer data across corporate networks undetected (Mehrnezhad, Toreini, Shahandashti & Hao, 2018).

The McAfee Mobile Threat Report reveals a troubling trend: over 65,000 fake apps have been detected, with their numbers increasing each year. In response to this growing threat, several tailored solutions have been developed to address mobile application attacks. Notable contributions include research by Diallo, Samhi, Bissyandé, and Klein (2024), as well as Gautam *et al.* (2023).

#### *4.1.4 Attacks and threats to mobile connectivity domain*

Mobile device connectivity enables devices to connect to the internet and each other through a range of wired and wireless methods. These include cellular mobile networks like 5G, Wi-Fi, Bluetooth, Near Field Communication (NFC), Universal Serial Bus (USB), mobile hotspots, infrared, and satellite networks (Meng *et al.*, 2018). One of the most widely adopted communication technologies is Bluetooth. According to Xu, Diao, Li, Chen, and Zhang (2019), once a Bluetooth device is paired with a host device, it can seamlessly exchange commands and data, including voice inputs, keyboard and mouse commands, and network connections. However, Bluetooth technology is not without its vulnerabilities. Attacks on Bluetooth can take various forms, such as bluesnarfing, bluejacking, and bluebugging (Sousa & Reis, 2024; Gunn *et al.*, 2022).

Sharma *et al.* (2024) highlights the growing prevalence of open access and public Wi-Fi in urban areas, where comprehensive coverage is increasingly available throughout municipalities. However, this convenience comes with significant risks. Cybercriminals often exploit unsecured or spoofed Wi-Fi networks to gain access to sensitive user data, including bank account details, emails, and social media profiles (Meng *et al.*, 2018; Zeadally, Sklavos, Rathakrishnan & Fowler, 2007). In addition to public Wi-Fi, mobile device hotspots—often referred to as tethering—allow one device to share its mobile data with another. Unfortunately, these hotspots are not immune to cyber threats. Attackers can carry out various types of attacks, such as "evil twin" attacks, where they create a counterfeit version of a legitimate access point to deceive users into connecting to a malicious network (Dahiya *et al.*, 2024; Tang *et al.*, 2020). Other common security threats include network spoofing, MFA fatigue attacks, improper session handling, and weak passwords (Sharma *et al.*, 2024; Rupprecht *et al.*, 2018). As reliance on open-access networks and mobile hotspots continues to grow, awareness of these vulnerabilities becomes increasingly crucial for users.

### 4.2 Future Research

The findings from the literature review indicate that security issues related to mobile device applications and websites are well addressed. However, while research primarily focuses on this domain, there is a need for further exploration into the areas of mobile device firmware and connectivity. A more comprehensive approach to securing mobile devices requires additional study of relationships across these domains. The literature review also highlighted various attacks that warrant further investigation within each domain. Future research should examine the controls and safeguards associated with each security issue. Additionally, there is a pressing need

to advance lightweight, real-time malware detection systems that can operate effectively on mobile devices with limited resources. This includes refining machine learning models to ensure they work efficiently on these devices while minimising battery consumption and processing demands. Recent advancements in deep learning and neural networks offer exciting possibilities for developing more resilient systems that can adapt to the evolving tactics of malware. Future studies may explore the optimum balance between effective malware detection and reduced data collection, thereby protecting user privacy while maintaining security standards.

## 5. Conclusion

Security issues related to mobile devices have significant consequences for individuals, groups, governments, and businesses. This study reviewed and analysed 32 articles, and the findings were categorised according to four critical elements of mobile device security: the mobile operating system, firmware, applications and websites, and connectivity. The analysis indicates that many security concerns remain unaddressed when it comes to protecting mobile devices. While a few articles focused on security issues related to mobile operating systems and firmware, the majority concentrated on applications and websites; consequently, most proposed solutions are found within this domain. Future research should emphasise the necessity and significance of systematically addressing all aspects of mobile device security to ensure a thorough approach. This systematic literature review has implications for both theory and practice. Theoretical implications include enhanced understanding of the mobile device phenomenon, as well as the expansion of security concepts associated with mobile devices through the proposed classification scheme and definitions. Practically, the findings from this study can assist inventors and developers in creating new security measures for mobile devices. Future research should prioritise the implementation of controls and safeguards associated with each security issue. It is vital to advance the development of lightweight, real-time malware detection systems that can operate effectively on mobile devices with limited resources. This requires a committed effort to refine machine learning models to ensure their efficient performance on these devices while reducing battery consumption and processing demands.

## References

Ahvanooey, M., Li, Q., Rabbani, M. & Rajput, A. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *International Journal of Advanced Computer Science and Applications*. Volume 8 issue number 10, 48550/arXiv.2001.09406.

Alepis, E. (2019). Notify this: Exploiting android notifications for fun and profit. In *Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, Funchal-Madeira, Portugal, January 22-24, 2018, Revised Selected Papers 4* (pp. 86-108). Springer International Publishing.

Alotaibi, S. D., Alabduallah, B., Said, Y., Hassine, S. B. H., Alzubaidi, A. A., Alamri, M. & Majdoubi, J. (2024). Bioinspired artificial intelligence based android malware detection and classification for cybersecurity applications. *Alexandria Engineering Journal*, *100*, 142-152.

Alure, S. & Puri, R. (2021). Firmware designing for Android Mobile. *International Journal of Advance Scientific Research & Engineering Trends*, volume *5 issue* 12, ISSN 2456-0774.

Arunakumari, B. N., Shrivathsa, P., & Vinodkumar, G. (2022). Attack and Defense Methodology Against the Share Intents in Android. In *Sustainable Technology and Advanced Computing in Electrical Engineering: Proceedings of ICSTACE 2021* (141-152). Singapore: Springer Nature Singapore.

Bhavan, A. V. S., Golla, S., Poral, Y., Paul, A. S., Honnavalli, P. B., & Supreetha, S. (2024). Android malware detection: A comprehensive review. *Research Advances in Network Technologies*, 41-82.

Bubukayr, M. A. S., & Almaiah, M. A. (2021). Cybersecurity concerns in smart-phones and applications: A survey. In *2021 international conference on information technology (ICIT)* (pp. 725-731). IEEE.

Dahiya, R., Kashyap, A., Sharma, B., Sharma, R. K., & Agarwal, N. (2024). Security in Mobile Network: Issues, Challenges and Solutions. *EAI Endorsed Transactions on Internet of Things*, *10*. doi: 10.4108/eetiot.4542

Debnath, N., & Jain, A. K. (2024). A comprehensive survey on mobile browser security issues, challenges and solutions. *Information Security Journal: A Global Perspective*, *33*(5), 593–612. https://doi.org/10.1080/19393555.2024.2347256

Diallo, A., Samhi, J., Bissyandé, T., & Klein, J. (2024). Security of Mobile Apps in Developing Countries: A Systematic Literature Review. *arXiv preprint arXiv:2405.05117*.

Doreswamy, H., Lokhande, M. & Uttam, R. (2021). Perception Analysis on using Computer Applications- A study on AAROGYA SETU App. *Paripex Indian Journal of Research*. 81-84. 10.36106/paripex/5709969.

Gautam, S., Pattani, K., Zuhair, M., Rashid, M., & Ahmad, N. (2023). Covertvasion: Depicting threats through covert channels based novel evasive attacks in android. *International Journal of Intelligent Networks*, *4*, 337-348.

Gimba, U. A., & Ariffin, N. A. M. (2024). Review on User Authentication on Mobile Devices. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *46*(2), 26-36.

Gunn, L. J., Asokan, N., Ekberg, J. E., Liljestrand, H., Nayani, V., & Nyman, T. (2022). Hardware platform security for mobile devices. *Foundations and Trends® in Privacy and Security*, Vol. 3: No. 3-4, pp 214-394. http://dx.doi.org/10.1561/3300000024

Hou, Q., Diao, W., Wang, Y., Liu, X., Liu, S., Ying, L. & Duan, H. (2022). Large-scale security measurements on the android firmware ecosystem. In *Proceedings of the 44th International Conference on Software Engineering* (pp. 1257-1268).

Hou, Q., Diao, W., Wang, Y., Mao, C., Ying, L., Liu, S. & Duan, H. (2023). Can We Trust the Phone Vendors? Comprehensive Security Measurements on the Android Firmware Ecosystem. *IEEE Transactions on Software Engineering*, *49*(7), 3901-3921.

Jing, X. O. (2021). Comprehensive Analysis and Development of Mobile Antivirus Application. Bachelor of Computer Science (Honours), Universiti Tunku Abdul Rahman. *https://orcid.org/0009-0004-4604-7143*

Kalyani, V. & Agarwal, A. & Sharma, H. (2020). A Deep Analysis of Cyber Security with Special Reference to the Effect of High-Speed Internet Connectivity on Smart Phones and User Privacy. *Journal of Management Engineering and Information Technology (JMEIT)*, Volume 7 issue 6. ISSN - 2394-8124. 10.5281/zenodo.4408564.

Kaspersky. (2024). Attacks on mobile devices significantly increase in 2023. https://www.kaspersky.com/about/press-releases/attacks-on-mobile-devices-significantly-increase-in-2023

Keteku, J., Dameh, G. O., Mante, S. A., Mensah, T. K., Amartey, S. L., & Diekuu, J. B. (2024). Detection and Prevention of Malware in Android Mobile Devices: A Literature Review. *International Journal of Intelligence Science*, *14*(4), 71-93.

Kralik, D., Visentin, K., & Van Loon, A. (2006). Transition: a literature review. *Journal of advanced nursing*, *55*(3), 320-329.

Leguesse, Y., Colombo, C., Vella, M., & Hernandez-Castro, J. (2021). PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone. *IEEE Access*, *9*, 168600-168612.

Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2018). Stealing PINs via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, 17(3), 291-313.

Meng, W., Jiang, L., Wang, Y., Li, J., Zhang, J., & Xiang, Y. (2018). JFCGuard: detecting juice filming charging attack via processor usage analysis on smartphones. *Computers & Security*, 76, 252-264.

Nawshin, F., Gad, R., Unal, D., Al-Ali, A. K., & Suganthan, P. N. (2024). Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey. *Computers and Electrical Engineering*, *117*, 109233.

Niveditha, V. R., & Ananthan, T. V. (2019). Detection of Malware attacks in smart phones using Machine Learning. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1).

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D. & Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *The BMJ*, *372*.

Rupprecht, D., Dabrowski, A., Holz, T., Weippl, E., & Pöpper, C. (2018). On security research towards future mobile network generations. *IEEE Communications Surveys & Tutorials*, *20*(3), 2518-2542.

Sharma, B. K., Walia, M., Sharma, Y., Beig, M. A., & Shukla, V. (2024). Advances and Challenges in Mobile Phone Forensics. In *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)* (pp. 1880-1886) IEEE.

Sousa, A., & Reis, M. J. (2024). 5G Security Features, Vulnerabilities, Threats, and Data Protection in IoT and Mobile Devices: A Systematic Review. *Evolutionary Studies in Imaginative Culture*, 414-427.

StatCounter Global Stats (2024). Mobile Operating System Market Share Worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide.

Sun, P., Garcia, L., Salles-Loustau, G., & Zonouz, S. (2020). Hybrid firmware analysis for known mobile and iot security vulnerabilities. In *2020 50th annual IEEE/IFIP international conference on dependable systems and networks (DSN)* (pp. 373-384). IEEE.

Sutter, T., & Tellenbach, B. (2023). FirmwareDroid: Towards Automated Static Analysis of Pre-Installed Android Apps. In *2023 IEEE/ACM 10th International Conference on Mobile Software Engineering and Systems (MOBILESoft)* (pp. 12-22) IEEE.

Tang, Z., Tang, K., Xue, M., Tian, Y., Chen, S., Ikram, M., & Zhu, H. (2020). {iOS}, your {OS}, everybody's {OS}: Vetting and analyzing network services of {iOS} applications. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 2415-2432).

Xu, F., Diao, W., Li, Z., Chen, J., & Zhang, K. (2019). Badbluetooth: Breaking android security mechanisms via malicious bluetooth peripherals. In *Network and Distributed Systems Security (NDSS) Symposium 2019*. ISBN 1-891562-55-X

Yao, J., & Zimmer, V. (2020). Building secure firmware. *Apress: New York, NY, USA*, 18-48.

Zeadally, S., Sklavos, N., Rathakrishnan, M., & Fowler, S. (2007). End-to-End Security Across Wired-Wireless Networks for Mobile Users. *Information Systems Security*, *16*(5), 264–277. https://doi.org/10.1080/10658980701747252.

Zhang, W., Wang, H., He, H., & Liu, P. (2020). DAMBA: detecting android malware by ORGB analysis. *IEEE Transactions on Reliability*, *69*(1), 55-69.

Zhu, H. J., Jiang, T. H., Ma, B., You, Z. H., Shi, W. L., & Cheng, L. (2018). HEMD: a highly efficient random forest-based malware detection framework for Android. *Neural Computing and Applications*, *30*, 3353-3361.