A Review of Smartphone as an Office: Security Risks and Mitigation Measures

Titus Muhambe Mukisa[1], Julius Murumba[2]

[1]*Maseno University, P.O. Private Bag, Maseno, Kenya*
[2]*The Technical University of Kenya, P.O. Box52428, Nairobi,00200, Kenya*

Abstract

Smartphones have become the most popular mode of communication as well as a novel mode of work, allowing users to work from anywhere and increasing their efficiency and responsiveness. However, the flexibility and convenience of mobile phones are associated with security risks. The objective of this study was to examine the threats and risks that smartphones face and to suggest mitigation strategies. A literature searches of scientific research articles published in online journals and databases was carried out. Some of the databases used are Google Scholar, IEEE Xplore Digital Library and Science Direct. The paper concludes that smartphones are not only capable of supporting office work but can also serve as a gateway to the Internet of Things (IoT) and a tool for user interaction with numerous electronic devices. This comes with concerns about technical threats associated with cybercrime, privacy infringements, and hidden data collection tendencies. The paper recommends advanced research to enhance counter-measures to mitigate the many existing security threats as well as those that may emerge in the future.

Keywords: *smartphone, office work, security threats, counter measures*

1. Introduction

Smartphone users can access a wide variety of services from their devices, including phone calls, internet access, data sharing and storage, online and offline games, mobile TV and radio, word processing, spreadsheets, and a host of other tools. Consequently, users' reliance on smartphones to perform a variety of activities and facilitate daily work practices has increased globally [1], [2], [3], [4], [5]. The use of a mobile office is an opportunity provided by smartphones and other apps; however, there are also many risks that must be considered. Few studies have focused on the security challenges presented by smartphone use for professional work and have proposed countermeasures. This review is necessary because the literature has not adequately addressed current and potential future threats and vulnerabilities. It highlights the utility of smartphones for personal, commercial, and professional purposes, and examines various risks, threats, and potential countermeasures. Our objective was to conduct a narrative review and evaluation of smartphone use as an office, its apps, security issues, and countermeasures, by reading and summarizing journal articles and online databases.

The topics covered in this paper are organized as follows: background information on current smartphone use and its potential for use as an office, mobile phone technology, smartphone use as an office, smartphone vulnerabilities and threats, and conclusions with countermeasures to vulnerabilities and threats. This study adds to the literature on smartphone technology advancements that offer opportunities for its use as a portable office and

Corresponding author: Julius Murumba *(j.murumba@gmail.com)*
Received: 20 March 2023; Accepted: 20 April 2023; Published: 24 April 2023

further synthesizes and analyzes threats and countermeasures to those threats.

Internet-enabled mobile devices such as smartphones, laptops, and PDAs are increasingly used to handle complex tasks. Office work, online shopping, banking, and networking through social media are examples of these tasks. The work of [6] and [7] revealed that businesses are under pressure from staff, customers, and external partners to use mobile phones and wireless technologies to access data and participate in meetings and official duties from anywhere. According to [7], mobile technology increases productivity by improving communication and enabling ubiquity. Consequently, traditional structures and business processes are transformed into ubiquitous functionality and virtual structures [6]. According to [4], a mobile phone is "a portable computing device that employs mobile communication technologies." Data, voice, and video can be transmitted wirelessly from a smartphone or other wirelessly capable devices using mobile communication technologies, without the need for a permanent physical connection.

Mobile phones are data transmission and reception devices that use digital or analog short waves [8]. A mobile multimedia device known as a "smartphone" combines the features of a phone with those of a portable computer, as well as an increasing number of other features such as sensors, electronic cameras, voice recorders, GPS navigation, and gaming consoles [9]. Smartphone users rely on a variety of applications, including business, online banking, e-mail management, and other business-related tasks, as well as leisure activities such as instant messaging, booking, maps, and other tools.

According to [3], as a result of workers' increased mobility and access to ICT, the nature of work and the workplace have changed, and work practices have diversified as a result of diffusion tendencies. Smartphones are increasingly being used to aid various aspects of office work. Telework, also known as distance work and flex work, which combines office and out-of-office work, is now common [3], [4]. Currently, smartphones function as networked computers, data storage devices, navigational aids, sound and video recorders, mobile banks, mobile doctors, photo galleries, and social network hubs. Therefore, they can increase the connectivity, productivity, mobility, and morale of those who work remotely.

Organizations and society continue to face novel and unforeseen challenges such as emergencies that call for immediate workplace activity responses, office accessibility issues, the option of working from remote locations, and situations such as the recent COVID-19 pandemic that require a remote operation. Consequently, smartphones have become indispensable tools that can function as mobile devices. Therefore, it is critical to address any potential flaws in network connections, mobile software, and hardware that can allow malicious and unauthorized device activities.

With the advancement of mobile technology and the availability of 4G services, new phenomena for business communication and data processing have emerged. Bring Your Own Device (BYOD) has become popular in business and enables workers to access organizational resources on their devices from both inside and outside the organization, depending on what they need for their jobs [6], [7]. The Bring Your Own Device (BYOD) evolved to include the security-risky concepts of Bring Your Own Technology (BYOT) and Bring Your Own Software (BYOS). Whether used for personal or professional purposes, mobile device use carries some risks that need to be minimized. Research in [10] and [11] showed that mobile devices are vulnerable to numerous security challenges and malicious threats. Because smartphones are Internet-based and contain personally identifiable information, hackers are enticed to launch more effective attacks owing to the lack of robust security mechanisms [9].

Mobile devices have particular operating systems that allow users to download and set up a variety of applications, also known as "apps," from online stores such as Google Play and the Apple App Store. According to studies [10] and [12], these apps improve the functionality of smartphones and their daily life. However, they are a source of malware that is disguised as normal applications [12]. Android, iOS, Microsoft Windows, and MacOS are the four most popular mobile operating systems [1]. Studies [13] and [14] Note that users typically download mobile apps and give out their personal information without giving security issues much thought in order to enable their newest smartphone generation to handle the various complex computational tasks.

2. Smartphone technology

Mobile phones are wireless handheld devices with voice and data services that benefit their users. Modern mobile phones are more frequently referred to as "smartphones" because they feature cutting-edge technologies such as sensors, GPS, and the ability to install apps. Thus, smartphones are essential components of the Internet of Things (IoT) and are the most commonly used devices in these environments because of smartphone-enabling technologies, such as built-in sensors, Bluetooth, RFID tracking, and near-field communication (NFC). A smartphone typically contains and transmits sensitive personal data, so using one poses serious security and privacy risks [15]. A smartphone can control IoT devices and serve as an IoT edge device, although it is generally regarded as a non-IoT device. A smartphone with multiple built-in sensors, such as GPS, cameras, accelerometers, gyroscopes, and wireless communication technologies, such as Wi-Fi, Bluetooth, and RFID, can play a significant role as an edge gateway [15].

There are three main components of mobile technology, as depicted in Figure 1, which include mobile hardware, mobile software, and mobility infrastructure, such as networks, delivery systems, and data transmission enabling technologies [6]. Mobile hardware refers to the actual mobile devices or device components that access or use mobility services. Mobile software consists of operating systems and software applications that users install on their mobile device. Telecommunication networks that are widely dispersed across a wide geographic area connect nodes on a wireless network to form a mobility infrastructure. There are numerous features available for today's mobile devices, some of which are preinstalled and others that can be added via carrier plans. There are numerous mobile phone providers, also known as "carriers," around the world [16].

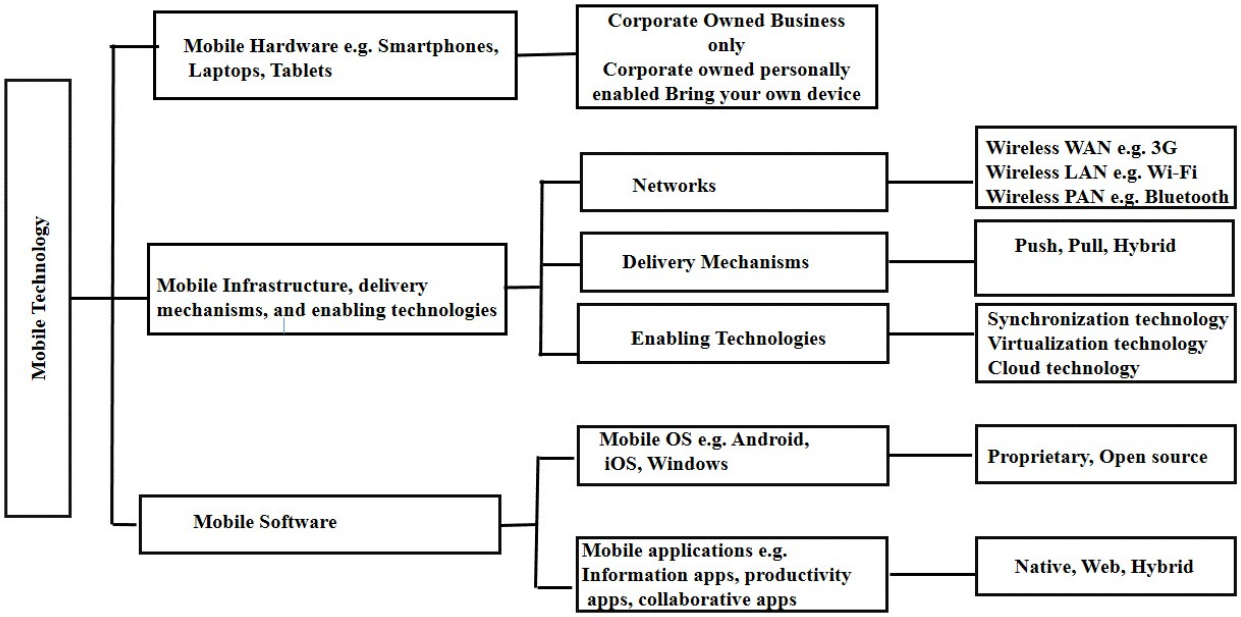

Figure 1. Core mobile components [6].

3. Smartphone as an office

Many people rely on smartphones in many aspects of their daily lives; as a result, they cannot live without them. The number of smartphone users has grown significantly owing to their widespread use as a mode of communication that enables the use of voice calls, text messages, emails, and social networking sites for entertainment. Digital cameras, music and video players, portable satellite navigation, e-book readers, voice recorders, paper diaries, personal organizers, and watches are just a few conventional products replaced by smartphones [13]. According to [17], a smartphone is a tool used by the user to perform any commonly accepted information processing, such as information gathering, organization, analysis, storage, and retrieval, as well as transmission and reception, processing, and display.

A smartphone combines mobile phones and computing capabilities into one unit, and can be used as a smart office. Thus, a "smart office" is an office setting that uses modern technology to improve worker efficiency, productivity, and experience through office environment optimization, while also remaining cost, and environmentally friendly. The foundation for having a mobile office on any smartphone is to combine several apps that can perform office tasks, such as mobile payments, social media, email, contacts, word processing, spreadsheets, and a camera. A smartphone fits all of this functionality into a user's pocket because of the miniaturized hardware that packs a processor, speakers, camera, GPS receiver, Wi-Fi adapter, and high-definition touch-sensitive screen into a cell-phone-sized device.

Table 1. Application areas of smartphone as an office.

Tool	Description
Word processing/Spreadsheet:	Used to create, review, and modify documents and spreadsheets.
Scanner	Mobile scanning applications, such as Genius Scan or Scanner Pro, can be used for scanning and printing.
Email management	A native email client on the device could provide email services The Outlook app can also be used to maintain a central list of recent file attachments to make it simple to operate on a mobile device.
Contacts/CRM	Native contact apps may be useful for basic information, whereas CRM apps such as SugarCRM and Batchbook are helpful for customer relations management.
Remote data access	This enables users to work on their smartphones and access files anywhere, such as Google Drive.
Time tracking	Users can easily keep track of their time with the help of a variety of time-tracking apps, such as Apploye, Clockify Time Tracker
Task and project management	Numerous mobile project management apps are available to assist project teams in managing their projects from anywhere e.g. oracle NetSuite, click up
Payments	Many mobile payment apps accept credit cards, such as PayPal, or use mobile money services, such as M-Pesa.
Mobile banking	Users can access their bank accounts using these smartphone applications at any time and location. Users can check their account balance, send money, pay bills, and perform other tasks by using a mobile banking app
Social media	These are smartphone-delivered social networking services, such as Facebook, Twitter, Instagram, Pinterest, and WhatsApp.
Expense tracking	A mobile application that aids in expense tracking. Expensify is an example of a platform that integrates accounting and ERP systems.
Camera	Smartphones are equipped with cameras to record both pictures and videos. In addition, the camera can be used for other things, like visual searches

Although smartphones were initially intended to be used for personal purposes, [17] claimed that, because of policies that permit or require their use, they are now also used for work-related activities. Smartphones have Internet access that allows people to do a variety of things with them, including access to social networks and knowledge sharing [17]. The primary applications of smartphones are information generation and communication with others, knowledge creation and sharing, and work-life balance. The workplace has changed, as has the nature of work. Telework, distance work, and flex work, which combine office and out-of-office work, are common [18]. This has been made possible by the widespread adaptability of mobile devices.

According to [6], there are two types of mobile enterprises: those that deploy mobile solutions primarily to increase productivity and improve communication and those that use technology to improve information quality, boost competitive advantage, and change business processes. According to [18], people can be mobile; they can work or operate from anywhere, and they can interact with others who are also mobile and working from anywhere using mobile tools. A smartphone can be fitted with the tools required to function as a mobile office that is capable of taking business and work from anywhere. Numerous work-enhancing applications can transform smartphones into mobile offices. Table 1 summarizes some apps.

4. Smartphone vulnerabilities and threats

The convenience of mobile technology has sparked widespread saturation, but its widespread use has serious implications for consumer safety [19], [14]. There are numerous security threats throughout the mobile phone environment. There are numerous security threats to the mobile phone environment. The key mobile components that these threats might try to compromise on are shown in Figure 1. While some may attempt to compromise the hardware of physical devices, for example, through theft, others may compromise mobile software, such as mobile operating systems or mobile apps, such as malware, and others may attempt to compromise the mobility infrastructure, for example, through denial-of-service attacks

Telecommunication networks, such as cellular or Wi-Fi networks, present vulnerabilities arising from the deployment or use of mobile devices [6]. Studies [11], [20] stated that the number of new mobile malware increased from 17000 in 2016 to 27000 in 2017, an increase of 54% increase in one year. Adware was the most prevalent mobile malware family in 2017, with the most significant increase in mobile threats. In the same report, greyware, or programs that are not malicious on their own but can cause data leaks, was the third most common mobile threat. Only 3% of Android mobile endpoints have the most recent operating system. 41% of these users used security patches that were two months old or older. Even with a more sophisticated update deployment platform, 20% of the iOS devices operate on out-of-date operating systems. Risky Wi-Fi connections, a little-noticed mobile threat, increased by 56% on average. Despite the fact that numerous significant malware attacks have been documented, the majority of users are still unaware of the necessary precautions [14].

Owing to the widespread use of mobile technology, using a smartphone as an office for business poses new and serious risks. Mobile phishing, iOS device hacking, and threats related to risky apps like AndroidSystemTheme are all too common. Because of their popularity, portability, and precarious security, smartphones and tablets are appealing targets for cybercriminals. Smartphone security risks are as follows:1) Theft or Loss, 2) malware, 3) Network Threats, 4) Denial of Service, 5) break-in, 6) Mobile App Threats, and 7) device cloning. There are malicious mobile applications that harvest data and can host remote command functionality in mobile software to create vulnerabilities [6], [21], [22]. Table 2 presents a summary of the smartphone vulnerabilities and threats.

Table 2. Smartphone Vulnerabilities and Threats.

Security Risk		Description
Vulnerability	Theft or Loss	- Being highly portable, the smartphone is exposed to risk of getting lost or stolen
	Phone /Data Services	- Risk to call eavesdropping or packets sniffing - Risk of exposure to unauthorized access - Risk of being be rooted or jail broken
	Malware	- Viruses, worms, Trojan horses, spyware, and grey ware are some examples of possible threats. - It can change or expose personal information on a smartphone - It can misuse the features and services of a smartphone, such as sending an SMS or MMS at random. - It may result in the smartphone being unavailable. For example, arbitrary code execution can render the device inoperable.
	Break in	- An attacker can gain partial or full control over a target smartphone using a flaw of code, code injection, or abuse of logic errors. - Device cloning, keystroke logging, and jailbreak software may be used to attack smartphone
	Denial of Service	- An attacker can risk availability of smartphone using radio interference
Threats	Mobile App Threats	- These are innocent looking but potentially harmful apps that could put users, user data, or devices at risk.
	Web-based threats	- Visiting some sites can result in malicious content being downloaded onto devices
	Wireless Network Threats	- A smartphone can be enticed to accept a Bluetooth or Wi-Fi connection that turns out to be malicious and intercepts all data sent or received by the connected devices. - Sniffing, spoofing, or eavesdropping on a wireless network to corrupt, block, or modify information

5. Counter measures to vulnerabilities and threats

Inadequate knowledge of mobile technology, coupled with the speed of new innovations and mobile technologies, has resulted in a lack of governance policies and practices. Owing to the rapid pace of innovation and revolution in the mobile technology landscape, mobile technology governance is typically implemented as an ad hoc reactive process to reduce risks as they arise, rather than a proactive strategy that appropriately aligns and governs the entire technology [2]. However, many of these risks have not been adequately mitigated.

The diversity of mobile technology complicates the implementation of control. According to [20] reports, 23% of iOS devices and 80% of Android mobile devices do not run the most recent operating system, making them susceptible to a sizable portion of malicious apps that are typically run on older operating systems [11], [23] Updates to installed operating system and software are critical. Security patches must be regularly applied to mobile operating systems and built-in applications.

Additional precautions must be taken, such as the following: 1) Phone settings and add-on utilities provide protection. 2) Refraining from rooting or jail-breaking operating systems. Although some advanced users and developers may want to remove operating system restrictions for their own personal freedom and preferences, all regular mobile users should exercise caution when doing so. 3) Avoiding risky apps. The official store e.g. Google Play Store / iTunes Store / App Store should be used for app installation on mobile devices. When apps are updated, they are fixed to previously detected vulnerabilities. 4) Maintaining physical control of the smartphone to avoid theft or loss [23]. 5) Cloud backup of data to enable recovery in cases of theft or loss.

According to studies [2] and [19], to comprehensively mitigate all risks, it is necessary to implement cross-cutting operational controls for mobile technology at the

component level. These include device control, communication, smartphone applications, software and data. A summary of the security practices is presented in Table 3.

The strengths and opportunities for using a smartphone for office work generate undeniable benefits. Table 4 summarizes the strengths, weaknesses, opportunities, and threats. A significant advantage of using a smartphone as an office is its accessibility to work documents, email, and social media, among other benefits. Similarly, using a smartphone as an office can offer users opportunities such as new business openings by utilizing cutting-edge technological innovations and trends. Some weaknesses and threats can pose security risks, limiting the use of smartphones for office work or professional work. Although most of these threats have countermeasures that, when used correctly, can mitigate them, there is a need for advanced research aimed at preventing emerging threats brought about by advances in mobile technologies.

Table 3. Counter measures to smartphone vulnerabilities and threats

Vulnerability/ Threat	**Security Practice**	**Description**
Theft/Loss	Physical Control of Device	- Maintaining physical control of the smartphone, especially in public places. Smartphones are small in size and can easily be misplaced or stolen
	Preparing for disaster recovery	- Insure phone - Record IMEI number - Enable remote lock and/or remote wipe features - Periodic testing of data backups
Denial of Service	Phone settings and add-on utilities	- Protection through phone settings and add-on utilities by o Enabling encryption o Enabling password protection o Disabling Bluetooth when not in use o Disabling GPS when not in use o Applying remote services: remote lock, remote wipe
- Malware - Mobile App Threats - Web-based threats	Anti-Virus Solution	- Install anti-virus solutions/ anti-malware o Malware can be prevented by using anti-virus software, as can access to phishing websites.
- Wireless - Network Threats - Break In	Avoidance of potentially harmful behaviors and activities	- Avoid the following o Downloading risky third-party applications o Connecting to known/trusted networks o Following links that are sent in suspicious email or text messages. - Keep your mobile phone number private. - Limit the personal data given to apps and websites
Theft/Loss	Cloud Backups	- Cloud Backups of data are important - If device is lost or stolen, user will be able to access any data that might have been compromised as quickly as possible
Phone /Data Services Risks	Avoiding “rooting” or “jail-breaking devices.	- Rooting your device exposes it to cyber threats. - Third-party device firmware can contain malicious code or unintentional security vulnerabilities

Table 4. SWOT Analysis - Use of smartphone for office/professional work

STRENGTHS	WEAKNESSES
- Ubiquity- Miniaturized hardware that is portable and has a high definition touch-sensitive screen, speakers, a camera, a GPS receiver, a Wi-Fi adapter, and a soap-shaped size that fits into a pocket. - Quick access to email, work documents and social media. - There are productivity apps including calendar, calculator, task manager, and GPS. - Optimization of agile business processes enabled - Can be used with IoT devices and has the ability to sync with other devices.	- Security concerns, such as the possibility that it could be stolen or lost easily because of its small size. - It contains a lot of personal and professional information, making it risky to hack and commit identity fraud if the phone is lost or stolen. - User Jail breaking or rooting their devices disables some of the operating system's built-in security features.
- Quick access to information in case of an emergency; for example, smartphone users can use their GPS to find their way if they are lost while driving. - New business models. i.e. the development of new business models that take into account emerging technology standards/trends, such as SMAC (Social, Mobile, Analytics, Cloud) for cloud data storage via mobile devices.	- Risk of malware, spyware, ransom ware - Users of smartphones are vulnerable to bandwidth bottlenecks, signal disruptions, Wi-Fi sniffing, Bluetooth-based attacks, automatic connectivity to insecure networks, and unauthorized device tracking. - Concerns about privacy, such as the ability to track a smartphone user via phone.
OPPORTUNITIES	**THREATS**

6. Conclusion

Smartphones have become an indispensable part of many global citizens' lives and are frequently used to perform office functions, exposing users to risks as new innovations emerge. This paper discusses smartphones, their potential use as offices, security risks and vulnerabilities, and available countermeasures. The smartphone is evolving beyond the capability to support office work, to serve as a gateway to the Internet of Things (IoT), and as a hub for user interaction with devices at home and work. This comes with concerns regarding privacy infringement and hidden data-collection tendencies. According to forecasts, there will likely be an increase in the technical threats posed by cybercrime on mobile devices. Similarly, a mobile malware threat known as pandemic mobile malware is predicted to emerge in the future, and may infect mobile devices via an improvised Wi-Fi network to circumvent corporate security measures.

The scope of this study, which focuses on security risks at a personal rather than societal level, specifically the use of a smartphone to cause security breaches, is likely to have limitations. For example, mobile devices can provide a platform for communication, planning, and sensory input for protesters, as was the case during the Arab Spring. The potential of smartphones to target control systems used in industries such as the health sector (e.g., pacemakers and insulin pumps) raises the possibility of problems. For the findings to be credible, the scope of this study can be expanded to include societal security challenges. This paper recommends advanced research in cyber security technologies for mobile devices aimed at improvement of counter- measures to mitigate against the numerous existing security threats as well as those likely to emerge in the future.

References

[1] P. Kalia, Y. K. Dwivedi and A. Acevedo-Duque, "Cellulographics: A novel smartphone user classification metrics," *Journal of Innovation & Knowledge,* pp. 1-4, 2022.

[2] T. Li, T. Xia, H. Wang, Z. Tu, S. Tarkoma, Z. Han and P. Hui, "Smartphone App Usage Analysis: Datasets, Methods, and Applications," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 2, pp. 937-965, 2022.

[3] D. Derks, A. , Bakker,., and M, Gorgievski,. "Private smartphone use during worktime: A diary study on the unexplored costs of integrating the work and family domains". *Computers in Human Behavior* , 114, 2021

[4] Ș. A Neștian,., S. M Tiță, and E. Turnea, S. "Using Mobile Phones at Work in Personal and Professional Information Processes". *Sustainability*, 12, 2020

[5] L. Li and T. T. C. Lin, "Smartphones at Work: A Qualitative Exploration of Psychological Antecedents and Impacts of Work-Related Smartphone Dependency,"

International Journal of Qualitative Methods, vol. 18, p. 1–12, 2019.

[6] M. Olalere, M. T. Abdullah, R. Mahmod and A. Abdullah, "A Review of Bring Your Own Device on Security Issues," *Sage Open,* pp. 1-11, 2015.

[7] A. Retnowardhani, R. H. Diputra and Y. S. Triana, "Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang," *TELKOMNIKA,* vol. 17, no. 2, pp. 753-762, 2019.

[8] V. Oksman, "The mobile phone: A Medium in itself," VTT Technical Research Centre of Finland, Vuorimiehentie, 2010

[9] W. Chmielarz, "The Usage of Smartphone and Mobile Applications from the Point of View of Customers in Poland," *Information,* pp. 1-13, 2020

[10] M. M. Engel, A. Ramadhan, E. Abdurachman and A. Trisetyarso, "Mobile Device Security: A Systematic Literature Review on Research Trends, Methods and Datasets," *Journal of System and Management Sciences,* vol. 12, no. 2, pp. 66-78, 2022.

[11] P. Weichbroth and Ł. Łysik, "Mobile Security: Threats and Best Practices," *Mobile Information Systems,* 2020

[12] A. Kumar and I. Sharma, "Understanding the Behaviour of Android Ransomware Attacks with Real Smartphones Dataset," in *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, 2023.

[13] A. Dominic, W. Ozuem and K. Howell, "Disruptive technology in the Smartphones industry: identity theory perspective". In A. Lupton, Leveraging computer-mediated marketing environments pp. 351-371. Pennsylvania, US: IGI Global, 2019.

[14] A. G. Chin, P. Little and B. H. Jones, "An Analysis of Smartphone Security Practices among Undergraduate Business Students at a Regional Public University," *International Journal of Education and Development using Information and Communication Technology,* vol. 16, no. 1, pp. 44-61, 2020.

[15] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi and R. Vera-Rodriguez, "A Survey of Privacy Vulnerabilities of Mobile Device Sensors," *ACM Computing Surveys,,* vol. 54, no. 11s, p. Article 224., 2022.

[16] E. Kroski, "Chapter 2: Mobile Devices," *Library technology reports,* vol. 44, pp. 10-15, 2008.

[17] Ș. A. Neștian, S. M. Tiță and E. Turnea, "Using Mobile Phones at Work in Personal and Professional Information Processes," *Sustainability,* p. 12, 2020.

[18] H. M. Zangana and M. Omar, "Threats, Attacks, and Mitigations of Smartphone Security," *Academic Journal of Nawroz University (AJNU),* vol. 9, no. 4, pp. 324-332, 2020.

[19] A. C. Cinar and T. B. Kara, "The current state and future of mobile security in the light of the recent mobile security threat reports," *Multimedia Tools and Applications,* 2023.

[20] D. Derks, A. B. Bakker and M. Gorgievski, "Private smartphone use during worktime: A diary study on the unexplored costs of integrating the work and family domains," Computers in Human Behavior , p. 114 , 2021.

[21] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," Telematics and Informatics , p. 55–69, 2019.

[22] S. Ozuomba, J. E. Akpasam and G. N. Ezeh, "Smart Phone Security Threats And Risk Mitigation Strategies," *Journal of Multidisciplinary Engineering Science Studies (JMESS),* vol. 8, no. 7, pp. 4585-4597, 2022.

[23] U. Thiruvaazhi and R. Arthi, "Threats to Mobile Security and Privacy," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 7, no. 4S, pp. 407-412, 2018.