Tuijin Jishu/Journal of Propulsion Technology
ISSN:1001-4055
Vol. 44 No.4 (2023)

A Review of Exploring the Distinctive and Contemporary Challenges in Safeguarding Mobile Devices.

Aaqib Nisar Bhat[*1], Irshad Ahmad Lone[2], Saba Tahir[3], Sajad Ahmad Shah[4], Shamim Ah hakeem[5]

[1]Research Scholar Computer Application Rimt University.
[2]Assistant Professor Govt Degree College Kulgam.
[3]Research Scholar Computer Application Arni University.
[4]Assistant Professor Govt Degree College Kulgam.
[5]Assistant Professor Govt Degree College Kulgam.

Abstract:

In recent years, cyber security has emerged as an issue that has the attention of individuals, organisations, and governments around the world. The fact that operating systems, networks, and the cyber domain are not completely safe presents users of these systems with a wide variety of obstacles to overcome. One possible explanation for the rise in cybercrime is that fewer people are aware of the nature of the threat. A large number of internet users automatically trust the security of the software and programmes they use. Other contributors to the rise in cyber insecurity include difficulties in integrating physical and cyber security as well as a lack of international collaboration in the fight against cybercrime. The proliferation of mobile devices and technological advancements has made the risk of cybercrime significantly more severe. Because mobile phone users are easy targets for hackers and other cyber-crime perpetrators, a new strategy is required in order to combat cyber insecurity brought on by the proliferation of mobile technology.

Keywords: *Cyber Security, Mobile Devices, Cyber Crime, Threat, Security.*

1. Introduction:

Mobile devices are the preferred communication tool in the 21st century. New technologies in mobile devices are being developed by the day. However, these developments relating to mobile technology devices expose owners of the devices to cyber insecurity. Mobile devices with internet connection options face a higher risk compared to those without. This assertion is supported by Drew. In his article, “Managing Cyber Security; Mobile and Cloud Open Doors to Opportunities and Threats”, Drew acknowledges the importance of mobile devices in connectivity. However, he maintains that people should not forget the imminent threat of cyber insecurity. Drew is objective in presenting his ideologies. His article presents a holistic view of the opportunities that mobile devices present and threats that accompany these opportunities.

Organizations permit employees to use their personal devices in the workplace. This is a common practice across all industries. However, this poses many security threats to individuals and the organization. One such threat is the risk of infiltration. A survey carried out by Dimensional Research on “The Impact of Mobile Devices on Information Security: A Survey of IT Professionals”, showed that organizations around the globe use mobile devices to connect corporate networks. The survey was carried out in different countries such as the

US, United Kingdom, Germany, and Japan. The survey is credible because it was carried out across different geographical locations and, therefore, data collected is a representative of the global situation.

Results from the survey support the position presented. It is globally accepted that employees can use personal devices in their work place. The survey also generalized that the android operating system installed in smart mobile devices posed a high risk compared to other operating systems (Dimensional Research). In addition, a key observation made from the survey is that over forty-seven percent of employees store company information and log in to company emails on their personal devices. This finding supports Drew's statement that employees use personal devices to access information that is sensitive to their organization. This leaves the organization vulnerable to external, malicious attacks. These two researches and Dimensional Researchare complementary. I agree with their recommendation that clear guidelines should be set in place to discourage use of personal devices in organizations.

According this introduction of smart phones, has increased the risk of cyber insecurity. In his article titled "CIOs Must Address the Growing Mobile Devices Security Threat", Johnson states that smart phones run on unsecure software that is highly susceptible to malicious attacks. An example of such software is the android operating system, identified by Dimensional Research as the most vulnerable operating system. Johnson maintains that hackers and malicious programmers can access any information stored in smart phones through hacking into the phones or use of Trojan horses. McClure & Scambray argue that hackers have perfected their skills and; therefore, users need to be aware of how to keep their mobile devices secure. Johnson's article is an eye-opener to people who use smartphones to store personal information. It explains the threats they face clearly and comprehensibly.

The paper "Technical Information Paper-TIP-10-105-01; Cyber Threats to Mobile Devices" by the United States Computer Emergency Readiness Team, provides a report on areas that users of mobile phones may encounter cyber-criminals. The report is realistic in that it addresses existing problems that every mobile device user faces. From the report, it is clear that inclusion of internet connectivity capability in mobile devices makes hacking easy. This is a serious issue that the government and the United States Computer Emergency Readiness Team (US-CERT) seek to address. One of the key objectives of US-CERT is to analyze threats and provide cyber security information to appropriate users. Therefore, users can rely on recommendations made in this report because it is from a credible source and publishing of reports is within the mandate of US-CERT.

2. Literature Review:

In his piece titled "Cyber Security," Amoroso (2007) draws the reader's attention to the risks associated with a lack of adequate online protection. The material written by Amoroso is very understandable and specific. It sheds light on the issue of cyber insecurity in all of its facets and describes the organizational flaws that contribute to increased cyber risk. He sees the violation of personal privacy as one of the primary risks that are posed by cyber-insecurity. In addition, the author discusses how simple it is for lawbreakers and those who commit acts of cybercrime to obtain personal information from members of the general public. He illustrates the gravity of the problem by linking the attacks of September 11th, 2001 to a lack of adequate cyber defences. According to his point of view, the terrorist assault that took place in the United States of America on September 11, 2001 was an instance of criminals exploiting technology and flaws in networks and systems. In a manner quite similar, Androulidakis (2012) divides the threats posed by a lack of cyber security into three distinct groups. These are dangers to integrity, confidentiality, and privacy all at once. Androulidakis discusses the methods that hackers and other cyber criminals use to conduct crimes online in his book titled "Mobile Phone Security and Forensics: A Practical Approach" (2012). This book is available on Amazon.com. These methods are also discussed in the book "Hacking Exposed: Network Security Secrets & Solutions" written by McClure and Scambray (2005). The authors detail a variety of ways in which users of information systems and gadgets put themselves in danger of being targeted by cybercriminals. McClure and Scambray (2005) provide an illustration of how the use of search engines like Google results in the possibility of assaults being launched on users.

Amoroso, (2007); Androulidakis, (2012); and McClure & Scambray (2005), provide detailed explanations of the general dangers the users of cyber systems face. All the authors are experts in fields related to cyber security. Amoroso worked as the Chief Security Officer in charge of Cyber Security for AT & T. On the contrary, Androulidakis has authored numerous books on forensics and cyber security. On this basis, their views provide an expert opinion on the dangers of cyber insecurity. The authors are in agreement that cyber-insecurity affects privacy, integrity and confidentiality of systems.

3. Measures to Curb Cyber Insecurity

The literature review above shows that mobile devices present enormous security risks to all users. The main issue of concern is that users of mobile devices are unaware of these threats, and, in most instances, fall to well-orchestrated cyber-attacks. Several authors have proposed measures aimed at ensuring cyber security. Their work is in line with the current study and provides solutions to cyber insecurity. Singer and Friedman's book, "Cyber Security and Cyber War; What Everyone Needs to Know" (2014), explains why it is necessary to adopt counter measures. The authors point out that a mobile device user's knowledge of cyber threats and cyber wars is vital. They also predict how cyber-crime will evolve in the future. The book is well structured and highly informative. Although the authors are from different academic backgrounds, they complement each other in addressing questions on cyber insecurity. Whereas Friedman is a renowned cyber expert and cyber security activist, Singer specializes in authoring books and articles on new warfare. Their partnership in authoring this book provides readers with diverse and elaborate information on why new measures should be adopted to fight cyber insecurity. The stories provided in the book make it engaging and enjoyable to read.

Similarly, Shoemaker and Conklin (2012) in their article titled "Cybersecurity: The Essential Body of Knowledge" discuss in detail the cyber security threat mobile device users face and propose several measures. The authors encourage users of mobile devices not to assume issues related to cyber security. This is similar to propositions made by Singer and Friedman (2014). Shoemaker and Conklin focus on creating awareness on the need for a global roadmap to address cyber insecurity. In my opinion, this is the easiest and surest way to address cyber insecurity. The vice can be eradicated through global cooperation. Shoemaker and Conklin believe that the establishment of a single global regulator will streamline the fight against cyber insecurity. The authors conclude that it is possible to curb cyber insecurity. They cite the example of Singapore, where cases of cyber insecurity have noticeably dropped after implementation of cyber security policies and regulations. Although Shoemaker and Conklin support the establishment of one organization to oversee cyber security, they contradict their views by encouraging national governments to implement national strategies to address the same issue. Their arguments are not evidence-backed, which makes them questionable.

Omar, Wright and Dawson, in their article "Cyber Security and Mobile Threats: The Need for Antivirus Applications for Smart Phones" (2012), propose simple measures to curb cyber insecurity. The authors believe that installation of antivirus software in Smartphones will reduce cyber insecurity. They argue that, unlike computers that have readymade antivirus programs, mobile devices are prone to cyber insecurity because only a few antivirus programs are credible. I agree with the authors' recommendation that manufacturers of mobile devices should incorporate build-in antivirus in the devices before taking them to the market. This will reduce the susceptibility of mobile devices to viruses and worms. The authors are scholars on cyber security. Wright works with the Florida Institute of Technology while Dawson works at the Alabama A & M University. Omar is a lecturer at the Colorado Technical University (Omar, Wright and Dawson, 2012). Their proposal is important to the study because it provides an economical solution to curbing a few internet threats. However, the authors do not address the root of the problem. Their solution is superficial because it does not affect perpetrators of cyber-crimes. In addition, cyber threats are changing by the day and antivirus programs become obsolete within a short time (Singer & Friedman, 2014).

In her article titled "Securing the Mobile Frontier" (2012), Fast identifies strategies that she believes will curb cyber insecurity. She acknowledges the need for awareness among all mobile device and internet users. Fast faults the government for being complacent with cyber-crime perpetrators. She also laments the ignorance of mobile device users. She states that users put themselves in danger of potential cyber-attacks through downloading insecure internet content or accessing unauthorized sites. She proposes that the government should put in place tough measures backed by stringent regulations to control cyber insecurity. She also points out that the responsibility of cyber security rests on every stakeholder. Therefore, it will take a combined effort of all stakeholders to curb cyber insecurity. Her sentiments are supported by Johnson (2012), who maintains that CIOs should actively participate in addressing mobile device threats. Similarly, Drew (2012) proposes that corporate executives must be a step ahead of cyber criminals in order to mitigate losses arising from cyber-crime. Fast (2012), Drew (2012), and Johnson (2012) carried out extensive research to support their points of view. Their opinion, therefore, is credible and qualitative, and users can rely on it.

The book, “Cyber War; The Next Threat to National Security and What to Do about It” by Clark and Knake (2010) contributes immensely to addressing cyber insecurity. The authors approach the issue from a different viewpoint compared to the authors discussed above. Clark and Knake consider the preparedness of the United States government on issues related to cyber war. The book brings to the reader’s attention that the government is doing little to curb cyber insecurity. This is in agreement with the statements made by Fast (2012). In addition, Clark and Knack argue that internet users ignore exploitation by cyber-crime perpetrators. They cite fear of ridicule and victimization as some of the factors fueling user ignorance. This makes it easy for internet criminals and spies to hide behind the anonymity of the internet (Clark & Knack, 2010). The authors’ suggestion that sound security programs be put in place to discourage cyber criminals is knowledgeable. The authors, Clark and Knack, are experts on national security. They use their experience in this field to identify various instances where national security has been compromised. They make it clear that government websites are not secure, which is alarming to the public.

4. Different Type of Mobile Security Threats

4.1. Social Engineering Threats:

Phishing and Smishing are two types of social engineering attacks in which malicious actors send bogus emails or text messages to your employees in an effort to deceive them into divulging confidential information such as their passwords or downloading malware onto their devices.

4.2. Data Leakage via Malicious App:

According to Dave Jevans, the Chief Executive Officer and Chief Technology Officer of Marble Security, "Enterprises face a far greater threat from the millions of generally available apps on their employees' devices than they do from mobile malware." This is due to the fact that 85 percent of smartphone apps available today are essentially insecure. The Chief Executive Officer of Appdome, Tom Tovar, has stated that "today, hackers caneasily find an unprotected mobile app and use that unprotected app to design larger attacks or steal data, digital wallets, backend details, and other juicy bits directly from the app."

4.3. Unsecured Public WiFi:

There is no way to find out who set up a public WiFi network, how (or if) it is secured with encryption, or who is now accessing it or monitoring it. As a result, the security of public WiFi networks is typically lower than that of private networks. The public WiFi networks that your employees connect to in order to access your servers (for example, from coffee shops or cafés) could pose a threat to your company as more businesses begin to provide telecommuting opportunities.

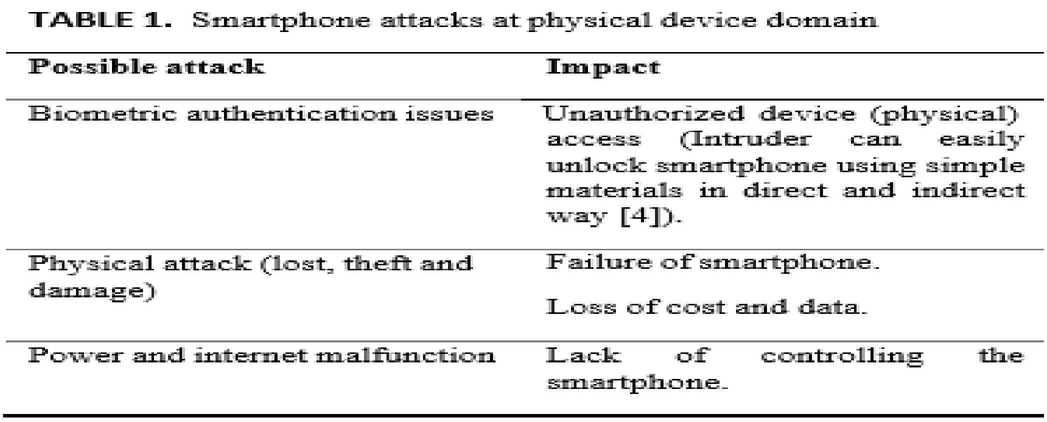


TABLE 1. Smartphone attacks at physical device domain

Possible attack	Impact
Biometric authentication issues	Unauthorized device (physical) access (Intruder can easily unlock smartphone using simple materials in direct and indirect way [4]).
Physical attack (lost, theft and damage)	Failure of smartphone. Loss of cost and data.
Power and internet malfunction	Lack of controlling the smartphone.

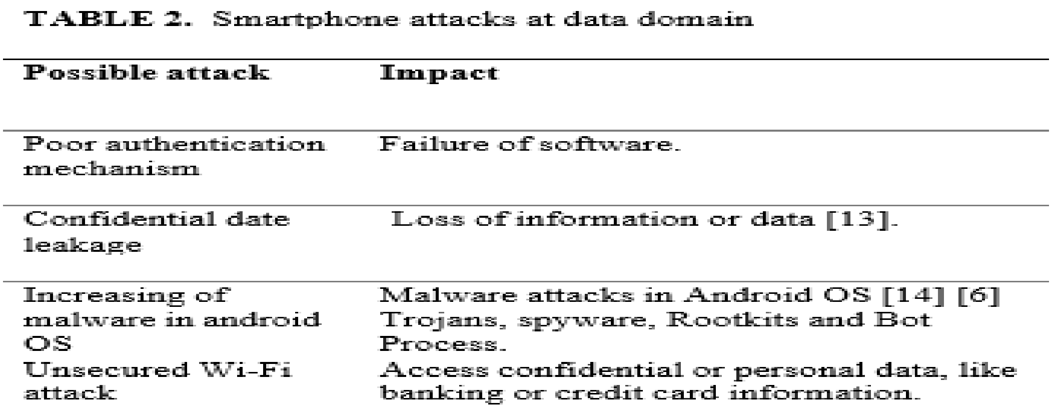


TABLE 2. Smartphone attacks at data domain

Possible attack	Impact
Poor authentication mechanism	Failure of software.
Confidential date leakage	Loss of information or data [13].
Increasing of malware in android OS	Malware attacks in Android OS [14] [6] Trojans, spyware, Rootkits and Bot Process.
Unsecured Wi-Fi attack	Access confidential or personal data, like banking or credit card information.

Fig.1 Cyber Security for Mobile network

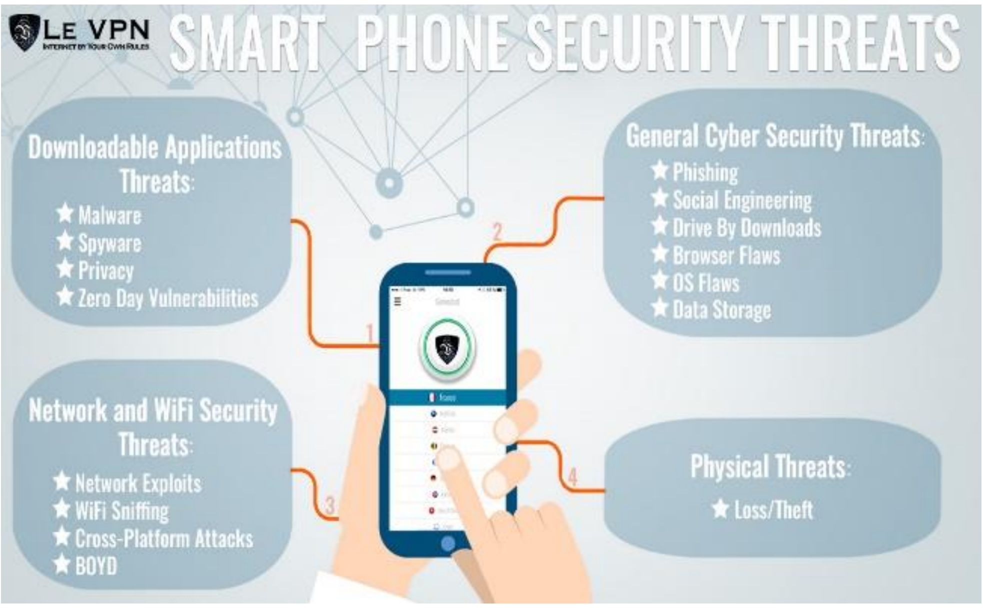


Fig.2 Security Challenges for Mobile Devices

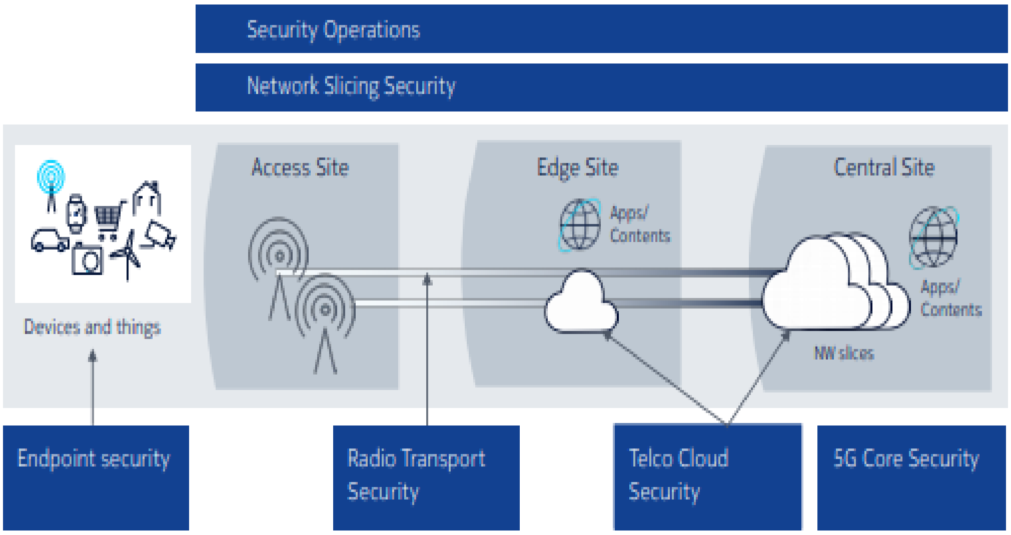
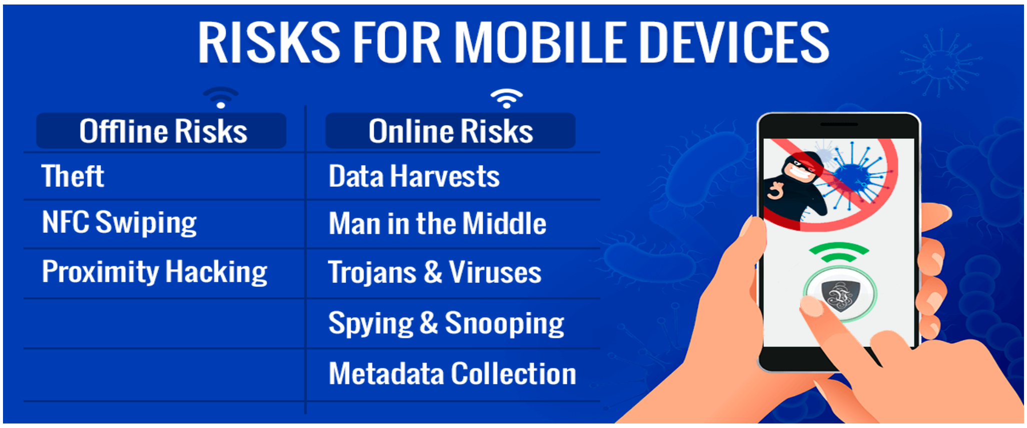


Fig.3 Risk for Mobile Devices



RISKS FOR MOBILE DEVICES

Offline Risks	Online Risks
Theft	Data Harvests
NFC Swiping	Man in the Middle
Proximity Hacking	Trojans & Viruses
	Spying & Snooping
	Metadata Collection

5. Conclusion:

Users and businesses alike stand to benefit from mobile devices thanks to the many options they bring. However, these gadgets are susceptible to being attacked via the internet. They do not have adequate safety measures. Hackers, phishers, and spies all take use of these security vulnerabilities in order to get unauthorized access to private information in order to commit acts of cybercrime. Mobile devices have been linked to an increase in the number of instances of cybercrime. It is imperative that drastic actions be done in order to combat the rising level of cyber insecurity. Among these are the raising of awareness among users, the development of antiviral software that is pre-installed on mobile devices, and the establishment of a global body with the authority to combat cyber vulnerability. In addition, in order to accomplish cyber security, there needs to be a concerted effort on the part of the government, corporate bodies, and individuals who utilise the internet and information system.

6. Conflict of Interest:

The authors of this manuscript declare that they have no conflicts of interest related to the research presented in this paper. No financial or personal relationships with other people or organizations have inappropriately influenced this work.

References:

[1] S. J. Alsunaidi and A. M. Almuhaideb, "Security Methods Against Potential Physical Attacks on Smartphones," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769458.

[2] D. Teixeira, L. Assunção and S. Paiva, "Security of Smart HomeSmartphones Systems," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 2020, pp. 1-5, doi: 10.23919/CISTI49556.2020.9141025.

[3] MadhaviLathaChalla and K.L.S.Soujanya, 2021. Secured smart mobile app for smart home environment. [online] Volume 37, Part 2(ISSN 2214-7853), pp.2109-2113. Available at: [Accessed 11 March 2021].

[4] Z. Zahid, A. Haider, N. Sabahat and A. Tanwir, "Vulnerabilities in Biometric Authentication of Smartphones," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-5, doi: 10.1109/INMIC50486.2020.9318094.

[5] Marion Lara Tan, Raj Prasanna, Kristin Stock, Emma Hudson-Doyle, Graham Leonard, David Johnston,Mobile applications in crisis informatics literature: A systematic review,International Journal of Disaster Risk Reduction,Volume 24, 2017, Pages 297-311, ISSN 2212- 4209, https://doi.org/10.1016/j.ijdrr.2017.06.009

[6] Yan, Ping. (2018). A survey on dynamic mobile malware detection. Software Quality Journal. 26. 1-29. doi: 10.1007/s11219-017-9368-4.

[7] Goel, Diksha& Jain, Ankit. (2017). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security. 73. doi: 10.1016/j.cose.2017.12.006.

[8] PMD Nagarjun and ShaikShakeel Ahamad, " Review of Mobile Security Problems and Defensive Methods," 2018 International Journal of Applied Engineering Research ISSN 0973-4562, Volume 13, Number 12 (2018) pp. doi: 10256-10259.

[9] Ibrahim Osman Adam, MuftawuDzangAlhassan, The effect of mobile phone penetration on the quality of life, Telecommunications Policy, Volume 45, Issue 4, 2021,102109,ISSN 0308-5961, doi.org/10.1016/j.telpol.2021.102109.

[10] Y. Wang, C. Hahn and K. Sutrave, "Mobile payment security, threats, and challenges," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1-5, doi: 10.1109/MOBISECSERV.2016.7440226.

[11] Ahmed, Lawal&Cavus, Nadire. (2019). DETECTION AND PREVENTION OF SOCIAL MEDIA CYBERCRIME AMONG STUDENTS. 3773-3779. doi: 10.21125/edulearn.2019.0977.

[12] Butler, Rika. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. Information and Computer Security. 28. 555-574. doi: 10.1108/ICS-01-2020-0016.

[13] K. Karimi and S. Krit, "Smart home-Smartphone Systems: Threats, Security Requirements and Open research Challenges," 2019 International Conference of Computer Science and Renewable Energies (ICCSRE), Agadir, Morocco, 2019, pp. 1-5, doi: 10.1109/ICCSRE.2019.8807756.

[14] FarisAuidAlharbi, Abdurhman Mansour Alghamdi, Ahmed S Alghamdi (2021). "A Systematic Review of Android Malware Detection Techniques". International Journal of Computer Science and Security (IJCSS), Volume (15): Issue (1): 2021.

[15] MiladTalebyAhvanooey, QianmuLi,Mahdi Rabbani, Ahmed Raza Rajput. (2017). "A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks". International Journal of Advanced Computer Science and Applications, 8(10), p.2017. doi: 10.14569/IJACSA.2017.081005.

[16] Niall, M. D., Rincon, B., Kang, S.: Yerima, P. Miller, S. Sezer and Y. Safaei, “Deep android malware detection. In: Proc. 2017. ACM Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, pp. 301—308 (2017).

[17] Theoharidou M., Mylonas A., Gritzalis D. (2012) A Risk Assessment Method for Smartphones. In: Gritzalis D., Furnell S., Theoharidou M. (eds) Information Security and Privacy Research. SEC 2012. IFIP Advances in Information and Communication Technology, vol 376. Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-642-30436-1_36.