Safeguarding Mobile Users from Violation by Third-party Apps

ARTICLE HISTORY
Received 17 September 2024
Accepted 23 October 2024
Published 7 January 2025

Vusumuzi Malele
Unit for Data Science and Computing School of Computer Science and Information Systems Vaal Campus, North-West University
Vanderbijlpark, South Africa
vusi.malele@nwu.ac.za
ORCID: 0000-0001-6803-9030

Kagiso Mphasane
Unit for Data Science and Computing School of Computer Science and Information Systems Vaal Campus, North-West University
Vanderbijlpark, South Africa
kagisomphasane@gmail.com
ORCID: 0000-0002-3538-0608

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025

V. Malele, and K. Mphsane, "Safeguarding Mobile Users from Violation by Third-party Apps", Latin-American Journal of Computing (LAJC), vol. 12, no. 1, 2025.

Safeguarding Mobile Users from Violation by Third-party Apps

Vusumuzi Malele
Vaal Campus, North-West University
Unit for Data Science and Computing School of Computer Science and Information Systems
Vanderbijlpark, South Africa
vusi.malele@nwu.ac.za

Kagiso Mphasane
Vaal Campus, North-West University
Unit for Data Science and Computing School of Computer Science and Information Systems
Vanderbijlpark, South Africa
kagisomphasane@gmail.com

***Abstract*—**Insecure third-party mobile applications (apps) can have a detrimental impact on mobile users in terms of information security and data privacy. Insufficient protection for third-party mobile apps platforms may result in harmful installations. The purpose of this paper was to make recommendations on guidelines for safeguarding mobile users from violations by third-party apps. In this regard, empirical data was collected through questionnaires developed to determine the necessary themes that led to the development of the recommendations. The findings showed that a large percentage of participants were not aware of basic security methods to safeguard themselves. Secondly, there is a need for increased confidence in data integrity protocols, and the necessity to ability for emphasizing strong availability controls and backup strategies for mobile users' continuous access to services. Since the findings align with the Confidentiality, Integrity, and Availability (CIA) triad framework, then the recommendations were made as an implementation strategy of the CIA triad for safeguarding mobile users against violation by third-party apps. Mobile users will benefit immensely from the recommendations as they empower them as the first defence against cybercrimes.

Keywords*—CIA cybersecurity, third-party apps security, third-party apps security*

I. Introduction

Nowadays, mobile devices are being used widely all over the world and the usage of mobile devices is growing significantly. The increase signifies the level of demand for good mobile services. Most of the latter services are provided by third-party apps. There is a vast range of sources regarding app stores from where users can easily install the apps. These would include the official app stores delivered from various platform providers, third-party stores, and a range of device manufacturers.

In a world where the mobile application market is constantly growing, new third-party applications (apps) and gadgets are being developed daily. It is critical to take great care while collecting and processing users' personal information. However, app designers rarely consider the suitable means for doing so, and as a result, unsafe applications are launched. In other words, app designers must always use secure-by-design principles.

On the other hand, most mobile users have social media app accounts which increases the lack of security in terms of the collection of personal user information. There are currently a lot of social media app subscribers in South Africa. For example, in 2023, there were 30,4 million Facebook users in South Africa which accounted for 49.6% of its entire population, of which 51.1% were women, the largest user group (9,4 million) were young people from 18 to 24 years of age [1]**.** Most of the app account subscribers tend to not know the type of data used willing or unwilling by such apps.

With a growing number of users having accounts in social media apps, mobile app users need to understand and apply some safety protocols when engaging with third-party as well as online apps. For example, there are concerns regarding the misuse of data by third-party organizations [2]. Users do not require risky permissions from third-party apps to fully operate their mobile devices; however, 60% of third-party apps demand risky permissions [2]. The latter is against the users' privacy and increases the cyber-security threats that users might encounter, thereby creating complications for the user. On the other hand, app designers should think of secure-by-design principles for assisting mobile users not to make a pathway and doorway for cybercriminals.

Cybercriminals may employ smart mobile devices as an attack tactic. Unsurprisingly, smart mobile device users underestimated the value of their collective identities to thieves and how these can be sold [3]. Cybersecurity awareness is the first defence strategy against the violation of being bullied by third-party app providers. In this regard, it is important to find out what mobile users understand about privacy against third-party apps and how it could be violated by third-party apps. Based on their understanding, what recommendations could be made to safeguard users?

Against this background, this paper presents recommendations for safeguarding mobile users from third-party apps. It differs from a mere Google search as it uses empirical data from the users. This paper uses the Introduction, Methodology, Results and Discussion (IMRaD) format. In this regard, the following section will be a Methodology section, then Results and Discussion. The conclusion is presented after discussion.

II. METHODS

The research design is the plan or structure for carrying out research; it also specifies the strategies and methods utilized to collect and analyze data [15]. The research design utilized in this paper is depicted in Fig. 1. This research design comprises three phases: (i) literature scoping – collect themes and concepts relevant to safeguarding the mobile users, (ii) survey – data collection and analysis phase, and (iii)

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.02

recommendations – data utilization phase. In this respect, mixed methods were adopted in this paper.

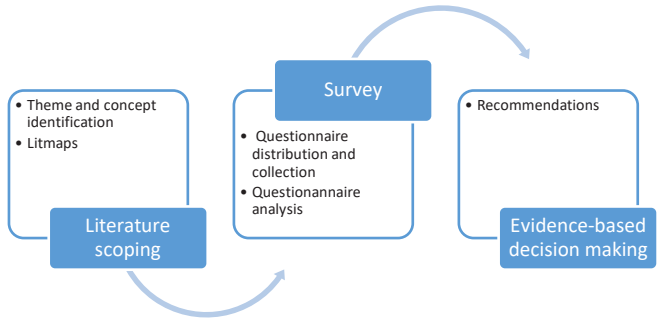

Fig. 1. The adopted research design (Source: Author)

A. Phase 1: Theme identification through literature scoping

To understand how mobile device users understand their devices, a literature scoping using Litmaps was conducted. A first seed literature article was selected and inserted in Litmaps. It generated a literature map that is illustrated in Fig. 2. The analyses of articles produced at least four themes that aim at safeguarding the mobile device against violation by third-party apps.

Fig. 2 produced cybersecurity themes that were relevant to this paper. The themes were within four broader areas: (i) governance – which looks at regulatory compliance requirements like the privacy of sharing the identification information; (ii) device management – which looks at how users operate their devices especially when they interact with third-party apps, (iii) authentication – looks at how the users access their apps; and (iv) data handling – looks at how users protect, keep and make data available always when they need it.

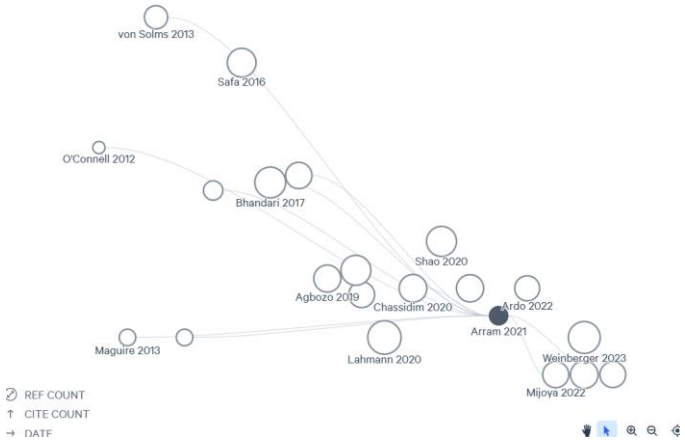

Fig. 2. A Litmap seed article for cybersecurity for safeguarding the user (Source: [5])

Using the CIA triad framework, questions of the questionnaire were designed from different reviewed literature [6–13]. Based on the latter broader themes, the CIA triad related questions were used to design the questionnaire as illustrated in Table 1 to Table 4.

TABLE I. GOVERNANCE QUESTIONNAIRE

Themes	CIA Triad	Questions
Governance	Confidentiality	Do you know what are security features of your mobile device through reading its user manual? Before downloading any app do you read its policies?
	Integrity	Do third-party apps force you to read the policy or memorandum of agreement before you use their app? Have you obtained any training regarding how you mobile device security features are?
	Availability	Do you use antivirus to protect your phone?
		Do you use update third-party apps after reading the guidelines?

TABLE II. DEVICE MANAGEMENT QUESTIONNAIRE

Themes	CIA Triad	Questions
Device Management	Confidentiality	Do you read and subscribe to the mobile device security guidelines before using the device? Do you read the mobile device security guidelines when you encounter security challenges?
	Integrity	Does the mobile device have different security settings available to the user? Can you locate the International Mobile Equipment Identity (IMEI) of your mobile device?
	Availability	When you download apps do you make sure that your device is always powered?
		Do you know more than one device that has the same apps?

TABLE III. PRIVACY THROUGH AUTHENTICATION QUESTIONNAIRE

Themes	**CIA Triad**	**Questions**
Authentication	Confidentiality	Do you unlock your screensaver with a PIN code or password? Do you keep your password and allow the system to recall it for you?
	Integrity	Do you use a Personal identification number (PIN) to

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.02

		unlock your Subscriber Identity Module (SIM)? Do you use a PIN/password or biometric identification to gain access to your mobile device?
	Availability	Do you change your password when prompt to do so or at certain time interval?
		Do you save or write your passwords somewhere else to make sure if you lost, you could withdraw it.

TABLE IV. DATA HANDLING QUESTIONNAIRE

Themes	CIA Triad	Questions
Data Handling	Confidentiality	Do you create a password, then lock and save your information? Do you read the third-party app guidelines before downloading the app?
	Integrity	Do you know what a re website cookies? Do you know how your data is handled by cookies?
	Availability	How often create backups of your information?
		Do you create different protected copies of your documents?

B. Phase 2: Empirical data through Survey

A research survey is a means of collecting data and analyzing it into information to get insight into a specific group of people. In this context, this study surveyed a sample of 120 participants who were randomly drawn from a significant study population made up of students (40), professionals (40), and unemployed people (40). All sample characteristics closely matched the population. Due to the issue of the timeframe, the questionnaire was distributed in person, and the participants were clarified about the purpose of the questionnaire and their right of consent (i.e. participants were given a chance to agree or disagree).

C. Phase 3: Evidence-based decision making

Research recommendations are suggestions or advice provided to guide a study and are obtained through action-based research or questionnaire-oriented research. They allow decision makers or researchers to provide manageable guidelines for achieving or solving the phrased problem. Research implications are broader than research recommendations.

Fig. 3 illustrates research recommendations vs the implications. Since the article aims at using the empirical suggestions through the collected data; then the aim of this paper was to provide the research recommendations through evidence-based decision making.

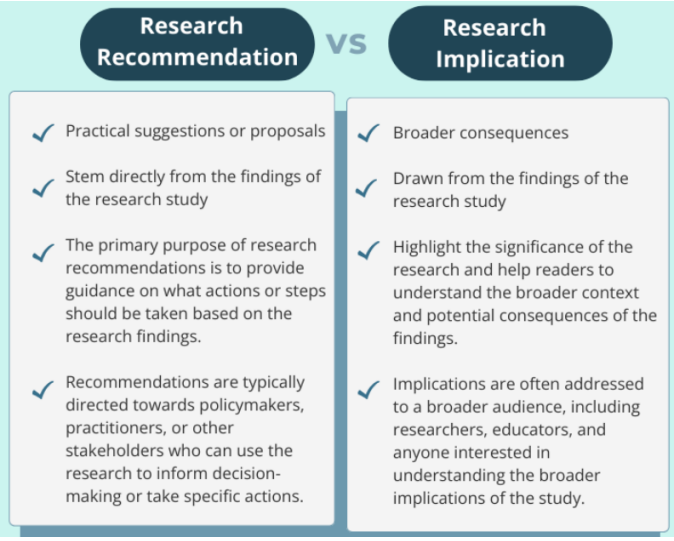

Fig. 3. Research recommendation vs research implications (Source: [17])

III. RESULTS AND DISCUSSION

A. Literature Scoping

Mobile apps are becoming an integral section of our daily lives [16]. With increasing dependence on apps, the major stakeholders for whom the data holds extensive value are the app providers, advertisers, and researchers. On this matter, through the analysis of the user data, the app providers could easily gain insights into the users' preferences and behavior [17].

Most studies that research mobile users' behavior, awareness, risk, ethics, and design use the Confidentiality, Integrity, and Availability (CIA) triad framework [6-11].

The CIA framework was adopted for this study because it elaborates on and strengthens mobile users' privacy through confidentiality, integrity, dependability and availability. In the context of CIA, confidentiality refers to privacy of Information and Communication Technologies (ICT), and the limitation of access to classified material and protecting private data or protection of sensible data about the users' livelihood [11].

While integrity refers to the knowledge that data or computing operations have not been corrupted or destroyed [11]. Furthermore, it describes the dependability of information and features offered by third-party apps [11]. Then, availability guarantees prompt and ongoing access to the system data for authorized app users [10].

Encryption is vital for information security but can also affect availability. If encryption is too strong or complex, it can slow down data access and processing, impacting system performance and availability.

The CIA framework will assist with a structure of recommendations that could be utilized for the protection of mobile users' Personal Identification Information (PII) data that could be accessed through mobile apps. In this context, the CIA triad was chosen as the theoretical baseline for examining the privacy and security risks that arise from third-party apps.

The CIA triad study conducted by [13] on mobile users regarding the PII showed that: (i) a large percentage of participants were confused about using a personal

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.02

identification number (PIN) or a password to access their screen savers; (ii) participants expressed concerns about the dependability of their data, and (iii) participants cited instances where they questioned the correctness of their PII, (iv) while others mentioned they suspected an unauthorized changes.

On the other hand, some researchers felt like there should be a move from CIA to a new theory [14]. They argue that information security is commonly defined and modelled using the CIA triangle; however, it is unable to deal with the quickly evolving need for security. In this regard, they proposed that the CIA triad should include the four layers and be called Confidentiality, Availability, Controllability, and Authentication (CACA). Unfortunately, CACA does not include digital mass surveillance, and it was not clear how CACA is used to target end users.

Although, the work by [18] explored information security usage of but the privacy and security of users when using third-party apps were not mentioned nor described by authors. Furthermore, no recommendation to safeguard users was made by [18].

The legal aspects of safeguarding mobile users against violation of mobile apps are another important matter. The work by [19] looked at privacy harm as a legal action caused by negative impact to an individual due to unathorised access. The legal solution led to the use of Privacy Enhancing Technologies (PETs) and implementation of privacy enhancement mechanisms (such as Fair Information Practice Principles (FIPPs), and Code of Fair Information Practice (CFIP)) to protect PII [19].

Interestingly, with increasing dependence on apps even operating systems (OS) are now offering privacy and access controls. The latter is achieved by amalgamating authentication between users file access to give file permissions as well as system monitoring. The work by [20] reveals that the CIA triad fuels OS security; it is at the heart of access control mechanisms, authentication protocols, encryption techniques, and secure coding practices. On this point, the OS security deals with system vulnerabilities, malware, insider threats, software flaws, and social engineering attacks. A protection framework has been contributed by [21]. It uses static and dynamic analysis, in addition to a review of privacy policy statements to improve the mobile OS (i.e. Android) security. The analysis protects the sensitive information for being collected by either public or private apps.

This paper adopted the CIA Triad to develop a questionnaire, which was then used it to collect the data. Then analyzed the data to produce a recommendation. The latter is summarized through the sections below.

B. Survey

The CIA triad of mobile users showed that [13]: (i) a large percentage of participants were confused about using a personal identification number (PIN) or a password to access their screen savers; and (ii) participants expressed concerns about the dependability of their data, citing instances where they questioned the correctness or suspected unauthorized changes. The empirical results of this study are shown in Fig. 4 to Fig. 7.

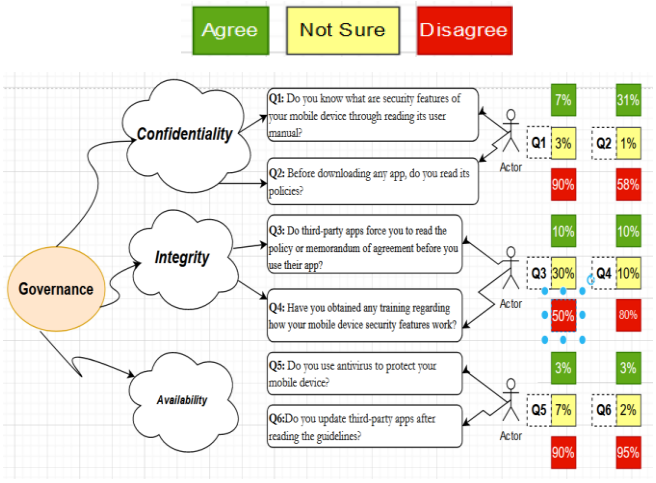

Fig. 4. Questionnaire response regarding cybersecurity governance as applied by mobile users

The issues regarding PII as acquired by third-party agencies beyond what is specified in the privacy and security policy have been gradually growing [15]. This means the growing user numbers lead to the growth, collection and capturing of PII data, stored in large amounts through mobile apps [18][22]. Consequently, mobile users are becoming concerned about how mobile apps acquire PII data [22]. However, the mobile users seem not adhere to the cybersecurity policies making them vulnerable to possible third-party app violation.

As illustrated in Fig. 4, the majority of mobile device users do not adhere to cybersecurity governance matters. In this regard, they become too exposed to the possibility of being attacked. For example, about 90% of the participants responded that they do not read any policies when coming them downloading third-party apps.

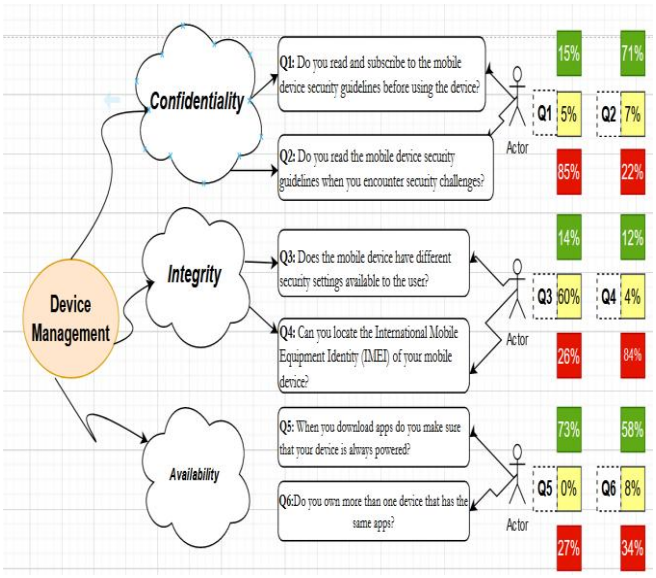

Fig. 5. Questionnaire responses regarding mobile device management

Fig. 5 illustrates the responses of mobile device owners in terms of their relationship or their understanding of device management. Most mobile devices could be used as a tool of

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.02

attack for cybercriminals. Unsurprisingly, mobile device users in the survey underestimated the value of their understanding of their device. For example, 85% of the participants responded that they do not read their devices guiding documents or manuals to enhance their stand of protecting the device. Furthermore, 73% of participants responded that they own more than two mobile phones for other people not to have their numbers, instead of blocking unwanted users.

Fig. 6 indicates that the majority of participants understand the authentication management in protecting their mobile devices. The authentication to access the mobile device is a must through a password. In alignment to Fig.7, most participants use a password to protect their documents. Unfortunately, the majority of users save their passwords on the device and allow the system to recall the password for them. The latter is a privacy thread as anybody who could access their password might use their PII and other privacy information.

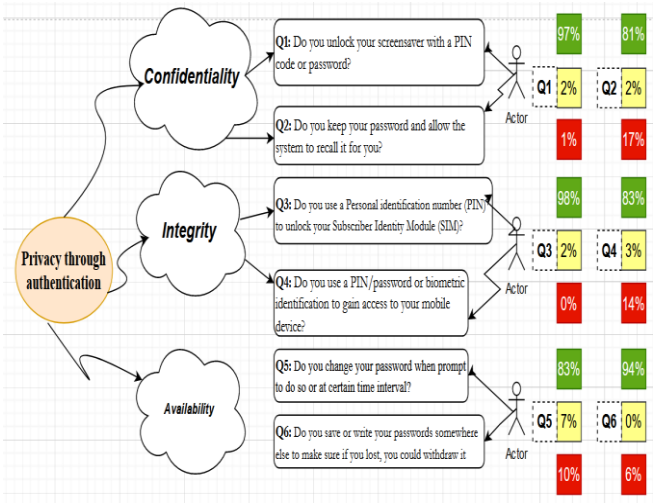

Fig. 6. Questionnaire responses regarding privacy through authentication

Fig. 7 illustrates how most mobile users handle issues relating to their data. Most participants have a redundancy plan to try and secure their data. In this regard, if one data set fails the original data could be available for re-used. Unfortunately, 51% users do not know what website cookies are; while 65% do not even know how cookies handle or use their data. Furthermore, most participants indicated that they do not read third-party app guidelines. The latter makes them vulnerable to third-party app organizations.

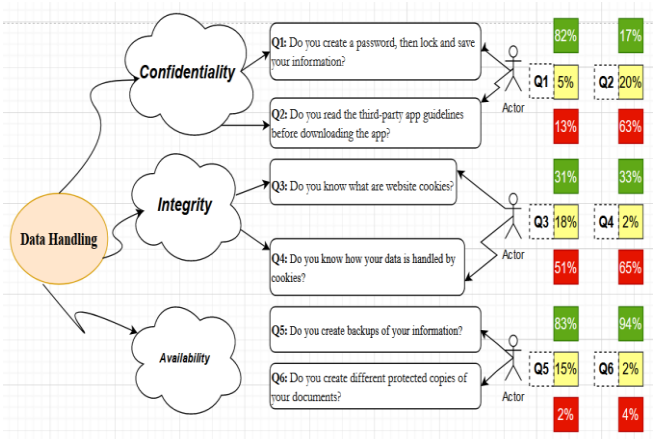

Fig. 7. Questionnaire responses regarding data handling

In general, most of the participants violated the CIA triad when coming to not using antivirus, backing their data and storing passwords in their same phones. The latter increases the chances of being vulnerable to violation by third party apps because their data is not secured. In this context, the following recommendations are contributed:

- Adhere to privacy policies and device management document – This can be done by providing the users with clear guidance on setting strong passwords, staying away from suspicious links and downloads, and using lock screen protection.
- Read about privacy and cybersecurity awareness and policies – awareness enhances a security-conscious culture among people. It helps minimize the human factor in security breaches and encourages people to be aware of their situation.
- Promote and practice privacy – user should promote, and practice promote privacy to avoid data leakage and superfluous permissions which could result in the release of personal information. While some of the flaws may be related to the system liberty, portability, and ease of use.
- Never rely of third-party apps for privacy and security guidance – Third-party tools should make sure that their data gathering policies are transparent to users. However, users should have more insight in reading the third-party application.
- Implement strong authentication and authorization – Implementation of strong authentication and authorization mechanisms is vital in hindering the unlawful access to the data in an app and its functionalities. The use of OAuth 2.0 and OpenID Connect is essential in ensuring secure authorization and therefore its implementation would ensure mobile security.
- Participate in user Education – although there was widespread knowledge of the importance of security measures with respect to password protection; however, users should be taught the best security practices and the possible risks related to mobile app usage.

IV. Conclusion

The rise of third-party apps raises concerns about privacy and security. This study employed the CIA triad theoretical framework to investigate and assess privacy issues related to third-party mobile applications that collect and share personal data from mobile users, with or without their agreement or understanding.

Mobile device users should be aware of how third-party apps acquire personal information. Furthermore, issues awareness regarding cybersecurity should not be ignored and it should always be emphasized when users purchase the devices.

The major goal of this paper was to collect empirical data from users and use it to assist in making the recommendation that could safeguard the mobile device users. Future studies will look at testing and validating these recommendations.

ISSN:1390-9266 e-ISSN:1390-9134 LAJC 2025
DOI: https://doi.org/10.33333/lajc.vol12n1.02

REFERENCES

[1] Napoleoncat statistics. https://napoleoncat.com/stats/facebook-users-in-south_africa/2023/12/

[2] T. Michael. Data privacy and security: Why mobile apps are the new weak link. Infosecurity Magazine. 2019. https://www.infosecurity-magazine.com/next-gen-infosec/privacy-mobile-apps-weak-link-1-1/

[3] K. O'Loughlin, M. Neary, E.C. Adkins, S.M. Schueller. Reviewing the data security and privacy policies of mobile apps for depression. Internet interventions, 15, pp.110-115, 2019.

[4] A. Nair. Research Recommendations – Guiding policy-makers for evidence-based decision making. Enago. 2024 https://www.enago.com/academy/recommendation-in-research/

[5] J. Moreno, M. Serrano, E. Fernández-Medina. Main issues in big data security. Future Internet, 8(3), pp.44, 2016. https://doi.org/10.3390/fi8030044

[6] M. Talal, A.A. Zaidan, B.B. Zaidan, O.S. Albahri, M.A. Alsalem, A.S. Albahri, A.H. Alamoodi, M.L.M. Kiah, F.M. Jumaah, M. Alaa. Comprehensive review and analysis of anti-malware apps for smartphones. Telecommunication Systems, 72, pp.285-337, 2019.

[7] A. Mathur, G. Acar, M.J. Friedman, E. Lucherini, J. Mayer, M. Chetty, A. Narayanan. Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), pp.1-32, 2019.

[8] P. Maroufkhani, R. Wagner, W.K. Wan Ismail, M.B. Baroto, M. Nourani. Big data analytics and firm performance: A systematic review. Information, 10(7), p.226, 2019.

[9] W.P. Wong, H.C. Tan, K.H. Tan, M.L. Tseng. Human factors in information leakage: mitigation strategies for information sharing integrity. Industrial Management & Data Systems, 119(6), pp.1242-1267, 2019.

[10] B. Awojobi, J. Ding. Data Security and Privacy. Cybersecurity for Information Professionals: Concepts and Applications, 291, 2020.

[11] C. Tode. 5 legal issues that could impede mobile marketing's progress. Marketing Dive, 2023. Available at: https://www.marketingdive.com/ex/mobilemarketer/cms/news/legal-privacy/10035.html.

[12] M. Christian. Information security and privacy in a digital world: A human challenge. TUprints TU Darmstadt publication service, 2022. TUprints. https://tuprints.ulb.tu-darmstadt.de/21138/

[13] L. Yin, B. Fang, Y. Guo, Z. Sun, Z. Tian. Hierarchically defining the Internet of Things security: From CIA to CACA. International Journal of Distributed Sensor Networks, 16(1), 2020.

[14] C.K. Yee, M.F. Zolkipli. Review on Confidentiality, Integrity, and Availability in Information Security. Journal of ICT in Education, 8(2), pp.34-42, 2021.

[15] I. Yaqoob, I.A.T. Hashem, A. Gani, S. Mokhtar, E. Ahmed, N.B. Anuar, A.V. Vasilakos. Big data: From beginning to future

[16] W. J. Gordon, A. Landman, H. Zhang, D.W. Bates. Beyond validation: getting health apps into clinical practice. NPJ digital medicine, 3(1), pp.14, 2020.

[17] M. Talal, A.A. Zaidan, B.B. Zaidan, O.S. Albahri, M.A. Alsalem, A.S. Albahri, A.H. Alamoodi, M.L.M. Kiah, F.M. Jumaah, M. Alaa. Comprehensive review and analysis of anti-malware apps for smartphones. Telecommunication Systems, 72, pp.285-337, 2019.

[18] D. Trabucchi, T. Buganza, E. Pellizzoni. Give Away Your Digital Services: Leveraging Big Data to Capture Value New models that capture the value embedded in the data generated by digital services may make it viable for companies to offer those services for free. Research-Technology Management, 60(2), pp. 43-52, 2017. https://doi.org/10.1080/08956308.2017.1276390

[19] S. Herath, H. Gelman, L. McKee. Privacy Harm and Non-Compliance from a Legal Perspective. Journal of Cybersecurity Education, Research and Practice, 3(2), 2023.

[20] Z.B. Akhtar. Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques. International Journal of Advanced Network, Monitoring and Controls, 9(1), pp.

[21] D. Hayes, F. Cappa, N. A. Le-Khac. An effective approach to mobile device management: Security and privacy issues associated with mobile applications. Digital Business, 1(1), 2020.

[22] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, K. Beznosov. Android permissions remystified: A field study on contextual integrity. In 24th USENIX Security Symposium (USENIX Security 15), pp. 499-514, 2015.

AUTHORS

Vusumuzi Malele

Prof Vusumuzi Malele, well known as Vusi, is an Associate Professor of Computing including Information and Communication Technology (ICT) at the Vaal Campus of the North-West University. He holds a Doctor of Technology (DTech) degree in Industrial Engineering from Tshwane University of Technology (TUT). He is a senior researcher and postgraduate supervisor. His experience spans 25 years in the Computing and ICT fields, from being an adult schoolteacher, lecturer, researcher, engineer, and research manager. He specializes in Artificial Intelligence (AI), Cybersecurity, Data Science, Design Science, ICT for Development, ICT for Society, Internet of Things (IoT), Industrial Internet of Things (IIoT), Industrial and System Engineering, Software Engineering, Wireless Systems and Wireless Networking.

Kagiso Mphasane

Mr Kagiso Mphasane holds a Master of Science in Computer Science from the School of Computer Science and Information Systems (CSIS) at the Vaal Campus of the North-West University (NWU) as well as the CISSP and CompTIA Security+ certifications. He is a detail-oriented Information Technology (IT) Security Specialist with 10+ years of experience in designing and implementing security solutions for enterprise-level networks. His expertise spans from risk assessment, vulnerability management, and incident response. His research interest spans cyber-security for organizations and society especially with the ability to identify potential security threats and mitigate risks to protect organizational data and systems from cyberattacks; conducted regular vulnerability assessments and penetration testing to identify and address security gaps, reducing risks by 40%, developed and enforced security policies and procedures, ensuring compliance with industry standards such as PCI DSS, HIPAA and GDPR; manage incident response efforts, investigating and mitigating cybersecurity threats, minimizing system downtime; monitor network traffic and conducted real-time threat detection, preventing multiple cyberattacks and unauthorized access attempts.