Fake Transparency: When Mobile Apps Say One Thing but Do Another

ALEJANDRO PÉREZ-FUENTE, Privacy Engineering Research Group, University of Valladolid, Spain
PABLO-ABEL CRIADO-LOZANO, Privacy Engineering Research Group, University of Valladolid; Miguel de Cervantes European University, Spain
M. MERCEDES MARTÍNEZ-GONZÁLEZ, Privacy Engineering Research Group, University of Valladolid, Spain

Mobile apps are extensively used. Transparency about the use of personal data is a requirement, both from a legal perspective and from an ethical perspective: users should know what data is accessed by these applications and how it is treated afterwards.

Sharing sensitive information with third parties can result in negative consequences for the data owner due to biased algorithms. Consent is necessary, as well as awareness that this will happen; the right to fair information is violated otherwise, particularly for collectives such as minors, who cannot consent to this processing.

To help prevent these problems, we propose an audit system in which conflicts between declarations made to users and declarations that accompany the software executed on mobile devices are detected. Our thesis is that this is feasible and beneficial for end users, developers, and other agents involved in app preparation.

Keywords: Mobile apps, audit, transparency, user rights

Reference Format:
Alejandro Pérez-Fuente, Pablo-Abel Criado-Lozano, and M. Mercedes Martínez-González. 2025. Fake Transparency: When Mobile Apps Say One Thing but Do Another. In *Proceedings of Fourth European Workshop on Algorithmic Fairness (EWAF'25).* Proceedings of Machine Learning Research, 7 pages.

1 Introduction

Mobile devices have become instruments of daily use. They are used to communicate, surf the Internet, access banking services, social networks, manage agendas, handle medical consultations and procedures with public administrations, etc. Thanks to their almost continuous availability, they have become 'warehouses' of data and photographs or videos, some of which may include sensitive personal data[1]. These unquestionable advantages in terms of ease of use and convenience are accompanied by risks of which users are often not fully aware.

The General Data Protection Regulation, GDPR [19], requires privacy policies to adequately inform about the personal data that each application collects, for what purpose and with whom it shares it. This is known as the

[1] *Personal data* is defined in article 4 of GDPR as "any information relating to an identified or identifiable natural person ('data subject')"

Authors' Contact Information: Alejandro Pérez-Fuente, Privacy Engineering Research Group, University of Valladolid, Valladolid, Spain, alejandro.perez.fuente@uva.es; Pablo-Abel Criado-Lozano, Privacy Engineering Research Group, University of Valladolid; Miguel de Cervantes European University, Valladolid, Spain, pacriado@uemc.es; M. Mercedes Martínez-González, Privacy Engineering Research Group, University of Valladolid, Valladolid, Spain, mercedes@infor.uva.es.

EWAF'25, June 30–July 02, 2025, Eindhoven, NL

so-called duty to inform, set out in Articles 13 and 14 of the GDPR, which responds to the principle of 'lawfulness, transparency and fairness'. A problem is that these privacy policies are free-format texts. Some of them are long, difficult to understand [4]. This can be particularly worrying with disadvantaged groups in this regard: minors who have not reached intellectual maturity, people with reduced intellectual capacities due to education or health issues, or others.

More recently, Google has incorporated into Google Play a section called 'Data Safety' in which developers inform their users of the data they access [5]. Some researchers see it as a more readable alternative to privacy policies [12, 13]. However, in many cases, the information provided does not give app users a clear understanding about what data they share, for what purpose, and with whom they share this data. Generic data types are used, such as health and fitness information, which do not clarify the specific nature of the information collected.

Whatever the mechanism used by developers to inform their users about the data collected by their applications and how they use it, various studies show that these statements do not always correspond to reality [15, 20, 21]. This places users in a situation of helplessness. This also places the developers themselves in a situation of non-compliance with the duty to inform fairly (and to comply with the principle of minimality set out in Article 5 of the GDPR), which can lead to penalties.

Privacy concerns regarding mobile apps have been constant since their use became widespread [3]. These concerns range from the succinct access to personal data in applications used by particularly vulnerable groups [9, 14], the transfer and loss of particularly sensitive data such as health and other data [2, 6, 20], to the poor quality of the information provided to end users. Although positive steps have been taken in this direction, such as the introduction of the obligation to declare the data being collected, which we discuss in the Data Safety Section, there is still a need to provide users with mechanisms to assure them that this information is truthful and of high quality.

In order for parents to protect their children, or for healthcare professionals to recommend apps that respect their patients' right to privacy, they need accurate, quality information about the data these apps collect.

2 Privacy in Android mobile apps

The Data Protection Supervisors have issued several guidelines for providers of mobile apps to help them comply with regulations such as the GDPR [1, 7]. It is worth remarking that there can be several roles involved in the provision of a mobile app; for example, the persons who write the privacy policy can be legal experts, while the developers are technicians. There is the possibility of mismatches between the declarations made in privacy policies and what developers state if they fail to communicate effectively. This would ultimately mean that the information provided to end users is not as accurate and fair as it should be.

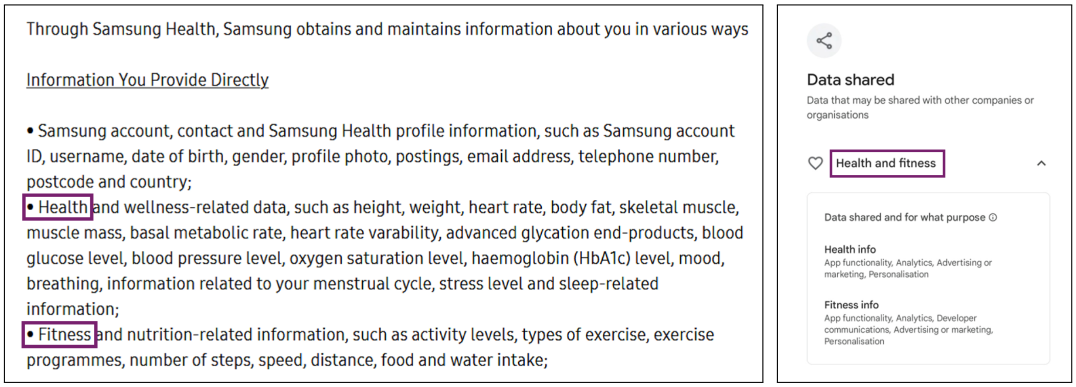
2.1 Data and permissions

Android implements a permissions mechanism that protects access to sensitive user data and critical system resources [16, 17]. To gain access, applications must request specific permissions. Applications declare the permissions they request in a file named `AndroidManifest.xml`. The operating system uses this file to learn about their requests and grant access to the resources accessible through those permissions. This file is the instrument used by developers to obtain the permissions to access user data. Users can grant or deny these permissions through their devices' settings. This is how users interact with apps to consent to access to their data. But do app users truly understand the implications of granting these permissions? Are they aware of what sensitive data they may be sharing with others? Ideally, they should be. Sensitive data, such as health data, when treated by biased algorithms, may be the base of harmful decisions, for example, being rejected for a job based on an apparent predisposition to suffer from a disease in the future.

2.2 Declarations to be consumed by end users in markets

Starting in April 2022, Google incorporated a section of information known as Data Safety into its marketplace for Android apps[2]. Until recently, it was optional for developers to provide this information. As of July 2022, it has become mandatory. The other source of information for end users is the privacy policy. The link to this document, which used to be lodged on developers' sites, is also available in app markets.

Figure 1 shows an extract of the Privacy Policy of an example app (Samsung Health), and the equivalent declaration in the Google Play Data Security section. This statement concerns access to users' health and fitness data. While the privacy policy explicitly mentions the collection of heart rate data, the corresponding section in Google Play only categorises it broadly under "health information" without specifying the type of data collected. This lack of specificity raises concerns about whether users relying solely on the Google Play disclosure are fully aware that their heart rate data is being collected.



Through Samsung Health, Samsung obtains and maintains information about you in various ways

Information You Provide Directly

- Samsung account, contact and Samsung Health profile information, such as Samsung account ID, username, date of birth, gender, profile photo, postings, email address, telephone number, postcode and country;
- Health and wellness-related data, such as height, weight, heart rate, body fat, skeletal muscle, muscle mass, basal metabolic rate, heart rate varability, advanced glycation end-products, blood glucose level, blood pressure level, oxygen saturation level, haemoglobin (HbA1c) level, mood, breathing, information related to your menstrual cycle, stress level and sleep-related information;
- Fitness and nutrition-related information, such as activity levels, types of exercise, exercise programmes, number of steps, speed, distance, food and water intake;

(a) Privacy Policy

Data shared

Data that may be shared with other companies or organisations

Health and fitness

Data shared and for what purpose

Health info

App functionality, Analytics, Advertising or marketing, Personalisation

Fitness info

App functionality, Analytics, Developer communications, Advertising or marketing, Personalisation

(b) Data Security Section Google Play

Fig. 1. Declarations to be consumed by end users.

2.3 Privacy issues and algorithmic fairness

Personal data are a potential source of discrimination. The harm is not in the data, but in the inappropriate use of this data. A risk that has increased with digitalisation and the powerful irruption of Artificial Intelligence. Some algorithms are capable of autonomously making decisions -without human intervention- based on their treatment

[2] https://support.google.com/googleplay/android-developer/answer/10787469?hl=en

of this data. In this section we will focus on some where apps play a decisive role, acting as agents that obtain and transmit the data used by algorithms in their decisions.

One group whose relationship with technology is of concern to legislators and society is that of children. Although they use gaming apps for entertainment, they are not mature enough to understand the implications that exposing their data can have. Some research has found that certain apps aimed at minors transmit their data to third parties [11]. There can be no informed consent to share such data on a minor.

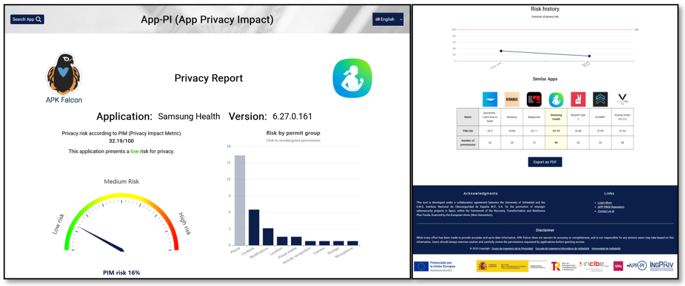
Another sector of particular concern is healthcare. The processing of health data has reached mobile applications, known as *mHealth*, raising concerns about the proper handling of this data. Some studies have revealed serious privacy issues and inconsistent privacy practices [2, 6, 8]. However, these inconsistencies are not limited to the healthcare sector [15].

Something similar occurs with female technologies. Numerous intimate data are collected. These data are processed, transferred, saved and shared with third parties [10, 18]. Once transferred to third parties, data owners do not have control on the type of treatment these data are fed to, whether fair or unfair.

3 Proposal

In the App-PI (*App Privacy Impact*) project, we start from the hypothesis that if users are provided with easy-to-understand and easy-to-use tools, it is much easier for them to become empowered to protect their privacy when using their mobile devices. To assist in this task, we designed an ecosystem in which users interact with services that allow them to check for conflicts between the information they receive and what happens to their data when a mobile application accesses it on their device. In this way, an application is audited from the perspective of its transparency and the quality of the information it provides to its users.

This tool can help developers to check their products. But it can also be the basis of user-oriented services that provide them with easy-to-understand information. For example, we have built one of these tools for our outreach activities with end users, *APK Falcon*[3]. Simple graphics and numerical indicators help users better understand the potential privacy risks associated with an app. Figure 2 shows the assessment of Samsung Health using this tool, where a bar chart highlights the relative weight of each user-controllable permission. Here, the "Phone" permission carries the most weight, and denying it—something users can simulate by interacting with the chart—significantly reduces the app's risk.



Application: Samsung Health Version: 6.27.0.161

Privacy risk according to PIM (Privacy Impact Metric)
32.19/100

This application presents a low risk for privacy.

Name	SwimtoFly - Learn how to Swim	Kenamju	Magna Me	Samsung Health	Beyond Type 2	ELEMNT	Viceroy Smart Pro 2.0
PIM risk	28.3	29.86	32.11	32.19	32.88	37.99	47.24
Number of permissions	24	25	15	99	20	20	38

Acknowledgments

This tool is developed under a collaboration agreement between the University of Valladolid and the S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. for the promotion of strategic cybersecurity projects in Spain, within the framework of the Recovery, Transformation and Resilience Plan Funds, financed by the European Union (Next Generation).

Disclaimer

While every effort has been made to provide accurate and up-to-date information, APK Falcon does not warrant its accuracy or completeness, and is not responsible for any actions users may take based on this information. Users should always exercise caution and carefully review the permissions requested by applications before granting access.

© 2025 Copyright: Grupo de Ingeniería de la Privacidad Escuela de Ingeniería Informática de Valladolid Universidad de Valladolid

Fig. 2. Assessing Samsung Health in APK Falcon.

[3] https://apkfalcon.inf.uva.es

Despite being a health app, Samsung Health receives a low privacy risk score. This is due to the assessment method, which prioritises permissions commonly exploited by malware—such as phone or location access—while health-related permissions are not yet ranked as highly [22].

This proposal is framed within an ecosystem that includes a quality metadata repository, which will provide the audit tools with the data they will use. Figure 3 shows the repository, called App-PIMD, and its interaction with the auditing tool.

Auditing consists of checking for conflicts between the statements that developers provide to users and those they provide to the operating system that will run the applications. In the Android world, the statements to users can come from two sources: (a) The privacy policies. (b) The statements available in the Data Safety section of the Android market, Google Play. On the other hand, the statements used by the Android operating system when running an application are found in the `AndroidManifest.xml` file, which accompanies the code that developers provide on Google Play.

Figure 3 shows the data flow for an example app, Samsung Health. In this figure, the audit process corresponds to the Verification Phase processes. The data used come from the App-PIMD repository, which stores the app metadata extracted from the various sources used for the audit. The outcome is a report with the results of the analysis.

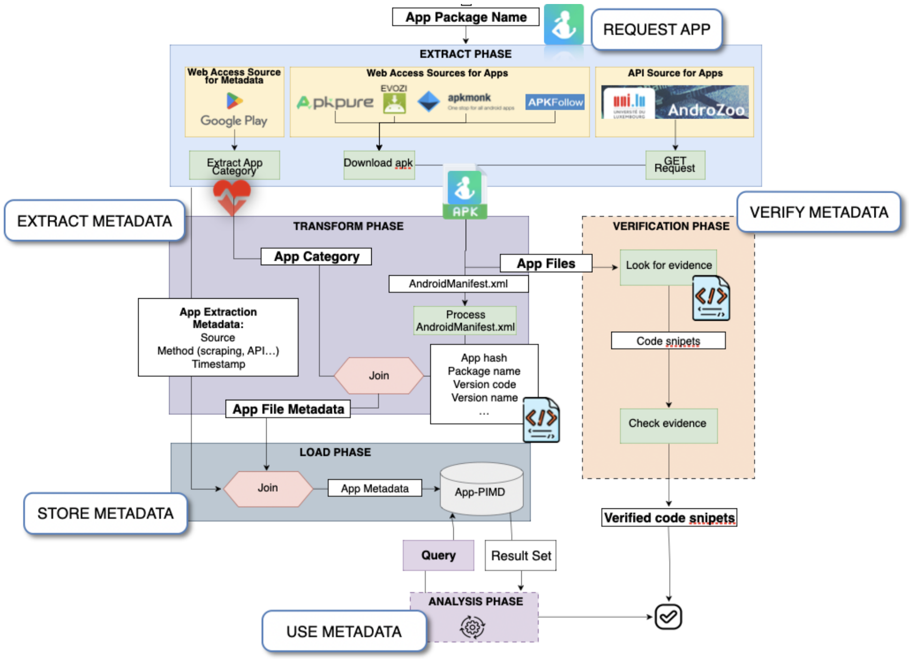


Fig. 3. Data flow until the audit checks for an example app.

4 Online Resources

The App-PIMD repository is available from https://app-pi.infor.uva.es/docs.

Acknowledgments

This work is included in the activities of the strategic Cybersecurity project "App-PI (*App Privacy Impact*): An ecosystem for the evaluation of the impact of apps for mobile devices on the privacy and security of their users", which is carried out under a collaboration agreement between the University of Valladolid and the Spanish National Institute of Cybersecurity (INCIBE) for the promotion of strategic Cybersecurity projects in Spain, within the framework of the funds of the Recovery, Transformation and Resilience Plan, financed by the European Union (*Next Generation*).

References

[1] Unidad de Evaluación y Estudios Tecnológicos. Agencia Española de Protección de Datos (AEPD). 2022. El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles. https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf.

[2] Md. Al Amin, Hemanth Tummala, Rushabh Shah, and Indrajit Ray. 2024. Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing. In *Proceedings of the 21st International Conference on Security and Cryptography, SECRYPT 2024, Dijon, France, July 8-10, 2024*, Sabrina De Capitani di Vimercati and Pierangela Samarati (Eds.). SCITEPRESS, 211–223. https://doi.org/10.5220/0012767400003767

[3] Jana Arbanas, Paul H. Silverglate, Susanne Hupfer, Jeff Loucks, Prashant Raman, and Michael Steinhart. [n. d.]. *Data privacy and security worries are on the rise, while trust is down. Deloitte's Connected Consumer Survey 2023.* Technical Report. Deloitte Center for Technology, Media & Telecommunications. https://www2.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html#

[4] Vanessa Bracamonte, Seira Hidano, Welderufael B. Tesfay, and Shinsaku Kiyomoto. 2020. User Study of the Effectiveness of a Privacy Policy Summarization Tool. In *Information Systems Security and Privacy*, Paolo Mori, Steven Furnell, and Olivier Camp (Eds.). Springer International Publishing, Cham, 186–206.

[5] Bostjan Brumen, Aljaz Zajc, and Leon Bosnjak. 2022. Permissions vs. Privacy Policies of Apps in Google Play Store and Apple App Store. In *Information Modelling and Knowledge Bases XXXIV, Proceedings of the 32nd International Conference on Information Modelling and Knowledge Bases, EJC 2022, Hybrid Event / Hamburg, Germany, May 30 - June 3, 2022 (Frontiers in Artificial Intelligence and Applications, Vol. 364)*, Marina Tropmann-Frick, Hannu Jaakkola, Bernhard Thalheim, Yasushi Kiyoki, and Naofumi Yoshida (Eds.). IOS Press, 258–275. https://doi.org/10.3233/FAIA220507

[6] James Burrell. 2024. Survey of Information Security and Privacy for Patient-Generated Health Data. *International Journal of Social Sciences and Public Policy* 6, 6 (2024). https://doi.org/10.33642/ijsspp.v6n6p1

[7] Commission Nartionale Informatique & Libertés (CNIL). 2025. Recommendation relative aux applications mobiles. https://www.cnil.fr/sites/cnil/files/2024-09/recommandation-applications-mobiles.pdf.

[8] Thomas Cory, Wolf Rieder, and Thu-My Huynh. 2024. A Qualitative Analysis Framework for mHealth Privacy Practices. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&PW 2024, Vienna, Austria, July 8-12, 2024*. IEEE, 24–31. https://doi.org/10.1109/EUROSPW61312.2024.00010

[9] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 314–335. https://doi.org/10.2478/popets-2020-0029

[10] Anna Ida Hudig and Jatinder Singh. 2025. Intimate Data Sharing: Enhancing Transparency and Control in Fertility Tracking. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 1184, 24 pages. https://doi.org/10.1145/3706598.3714089

[11] Lindsay Jibb, Elsie Amoako, Melissa Heisey, Lily Ren, and Quinn Grundy. 2022. Data handling practices and commercial features of apps related to children: a scoping review of content analyses. *Archives of Disease in Childhood* 107, 7 (2022), 665–673. https://doi.org/10.1136/archdischild-2021-323292 arXiv:https://adc.bmj.com/content/107/7/665.full.pdf

[12] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2024. Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section. In *33rd USENIX Security Symposium, USENIX Security 2024, Philadelphia, PA, USA, August*

14-16, 2024, Davide Balzarotti and Wenyuan Xu (Eds.). USENIX Association. https://www.usenix.org/conference/usenixsecurity24/presentation/khandelwal

[13] Julia Krämer. 2024. The death of privacy policies: How app stores shape GDPR compliance of apps. *Internet Policy Rev.* 13, 2 (2024). https://doi.org/10.14763/2024.2.1757

[14] Pierre Laperdrix, Naif Mehanna, Antonin Durey, and Walter Rudametkin. 2022. The Price to Play: A Privacy Analysis of Free and Paid Games in the Android Ecosystem. In *WWW '22: The ACM Web Conference 2022, Virtual Event, Lyon, France, April 25 - 29, 2022*, Frédérique Laforest, Raphaël Troncy, Elena Simperl, Deepak Agarwal, Aristides Gionis, Ivan Herman, and Lionel Médini (Eds.). ACM, 3440–3449. https://doi.org/10.1145/3485447.3512279

[15] Haoyu Liu, Douglas J. Leith, and Paul Patras. 2023. Android OS Privacy Under the Loupe - A Tale from the East. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2023, Guildford, United Kingdom, 29 May 2023 - 1 June 2023*, Ioana Boureanu, Steve Schneider, Bradley Reaves, and Nils Ole Tippenhauer (Eds.). ACM, 31–42. https://doi.org/10.1145/3558482.3581775

[16] René Mayrhofer, Jeffrey Vander Stoep, Chad Brubaker, Dianne Hackborn, Bram Bonné, Güliz Seray Tuncay, Roger Piqueras Jover, and Michael A. Specter. 2023. The Android Platform Security Model (2023). (2023). arXiv:1904.05572v3[cs.CR].

[17] René Mayrhofer, Jeffrey Vander Stoep, Chad Brubaker, and Nick Kralevich. 2021. The Android Platform Security Model. *ACM Trans. Priv. Secur.* 24, 3, Article 19 (apr 2021), 35 pages. https://doi.org/10.1145/3448609

[18] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In *CHI '21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, Yoshifumi Kitamura, Aaron Quigley, Katherine Isbister, Takeo Igarashi, Pernille Bjørn, and Steven Mark Drucker (Eds.). ACM, 409:1–409:11. https://doi.org/10.1145/3411764.3445132

[19] Official Journal of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[20] Abdelrahman Ragab, Mohammad Mannan, and Amr M. Youssef. 2024. "Trust Me Over My Privacy Policy": Privacy Discrepancies in Romantic AI Chatbot Apps. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&PW 2024, Vienna, Austria, July 8-12, 2024*. IEEE, 484–495. https://doi.org/10.1109/EUROSPW61312.2024.00060

[21] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kâafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. *The BMJ* 373 (2021).

[22] M. Upadhayay, A. Sharma, G. Garg, and A. Arora. 2021. RPNDroid: Android Malware Detection using Ranked Permissions and Network Traffic. In *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*. IEEE, 19–24. https://doi.org/10.1109/WorldS451998.2021.9513992