Assessing the Compliance of Mobile Applications with Personal Data Privacy Regulations: An Analytical Study

Ahmad Showail
Department of Computer Engineering, College of Computer Science and Engineering, Taibah University, Madinah, Saudi Arabia
ashowail@taibahu.edu.sa

Mohd Khaled Shambour
Department of Intelligent Systems Engineering, Faculty of Engineering and Design, Middle East University, Amman, Jordan
m.shambour@meu.edu.jo (corresponding author)

Hosam Jaradat
Department of Operating Systems, Deanship of Information Technology, Umm Al-Qura University, Makkah, Saudi Arabia
huss_kj@hotmail.com

Muhannad A. Abu-Hashem
Department of Geomatics, Architecture and Planning Faculty, King Abdulaziz University, Jeddah, Saudi Arabia
mabohasm@kau.edu.sa

Hani A. Aldhubaib
Department of Electrical Engineering, College of Engineering and Islamic Architecture, Umm Al-Qura University, Makkah, Saudi Arabia
hadhubaib@uqu.edu.sa

Received: 30 March 2025 | Revised: 3 May 2025, 15 May 2025, and 24 May 2025 | Accepted: 2 June 2025

 DOI: https://doi.org/10.48084/etasr.11214

ABSTRACT

The widespread use of technology has led to the need for data protection frameworks to regulate the collection, processing, sharing, and disposal of personal data. This study assesses the compliance of 66 Hajj and Umrah-related mobile applications with the Saudi Personal Data Protection Law (PDPL), focusing on applications available on Google Play and the Apple App Store. As a pioneering assessment in the religious tourism sector, this study examines the extent to which these applications meet the requirements of the PDPL, including consent, user rights, and data security. The findings show significant deficiencies in app developers' adherence to both user personal data requirements and user data protection principles, with compliance rates ranging from 18.2% to 33.3% and from 12.1% to 33.3%, respectively. These findings indicate the lack of data protection protocols in app development, underlining the vital need for developers to strictly adhere to personal data protection standards. The study emphasizes the crucial importance of preserving user personal information and encourages developers to prioritize data security, thus enhancing trust in the digital experiences of pilgrims.

Keywords-privacy; mobile applications; personal data; pilgrims; personal data protection laws

I. INTRODUCTION

With the rapid expansion of technology, applications have become essential tools for accessing services, especially in contexts involving sensitive user data such as health, identity, and location. This reliance on digital platforms raises serious concerns about data security, making strong regulations essential. In response, governments and organizations around the world have introduced strict frameworks to control how personal data is collected, stored, processed, and shared. These measures aim to address the growing ethical and legal challenges related to the widespread use of personal data. The General Data Protection Regulation (GDPR) of the EU [1], which was passed in 2016 and went into effect in 2018, is one of the laws that pioneered this field. The GDPR imposes severe fines of up to 4% of a company's worldwide revenue for non-compliance. For example, in 2019, Google was fined more than $50 million by the French data protection authority for violating user permission in ad personalization [2]. Similar to this, British Airways was fined more than £180 million for violating the GDPR due to data breaches involving passengers [3].

Regulatory authorities around the world have launched measures similar to the EU GDPR, building on its success. An example is the Virginia Consumer Data Protection Act (VDPA) [4]. In 2021, Saudi Arabia announced the protection of user digital privacy by enacting the Personal Data Protection Law (PDPL) [5]. This law sets strict rules for how organizations collect, store, and process personal data, with fines for violations of up to 5 million Saudi riyals (approximately USD 1.33 million) [5]. Its scope extends to everything from healthcare records to e-commerce transactions, but one area stands out with its unique challenges: Hajj and Umrah applications. In 2023, Saudi Arabia experienced a surge in tourist arrivals, totaling 109.34 million visitors, marking an astonishing 15.7% increase from 2022 [6]. Of these tourists, 27.42 million were international visitors and 81.92 million were domestic travelers. In particular, 19.5% of these individuals traveled to perform the Hajj and Umrah rituals.

Today, smartphones are widely used to connect users with various service providers, and it is estimated that there will be approximately 7.5 billion mobile customers worldwide by 2025 [7, 8]. This underscores the importance of stringent privacy policies to protect personal data. Several studies have investigated the compliance of mobile apps with international privacy laws, particularly the GDPR. In [9], 59 mobile applications were evaluated, finding that only a small fraction (14%) ensured secure data transmission. In [10], many apps were found to not disclose how they process user data. This highlights the urgent need for mobile apps across various sectors to prioritize transparent privacy policies and robust data protection measures to foster user trust and compliance with regulations.

In [11], the impact of GDPR on the privacy commitment of 50 top-ranked apps in Google Play was evaluated, observing an overall increase in privacy adherence compared to pre-GDPR levels. This study noted a significant decrease in privacy-related complaints following the enactment of the GDPR. Similarly, in [12], GDPR compliance was investigated among Android applications regarding the transfer and processing of personal data outside the EU. The findings revealed that 66% of the apps surveyed did not meet GDPR requirements. Furthermore, in [13], it was reported that 76% of the apps examined collected personal data from users insecurely, and 34% of them sent personal information to third parties. Free apps were significantly more aggressive in data collection than their paid counterparts [14], suggesting monetization through user data. In [15], a system was developed to automate the compliance process by converting legal requirements into actionable code. In [16], a GDPR-based design guide was presented to help developers integrate privacy principles into the application architecture. Other studies focused on user awareness and technological disclosure. In [17], user certainty about app permission requests was analyzed in the UK, finding half of the respondents uncertain about app privacy settings. To examine compliance with app privacy policies in cloud and fog environments, a machine-learning technique was introduced in [18] to detect the type of encrypted data shared by apps with external organizations, achieving an accuracy of 86%.

Although previous studies have provided valuable insights into app privacy and compliance with global frameworks, such as the GDPR, they have primarily focused on public or commercial applications in broader international contexts. There is a notable gap in studies on the compliance of applications with region-specific data protection laws, such as the Personal Data Protection Law (PDPL) in Saudi Arabia, particularly in areas that handle sensitive data, such as religious tourism. Hajj-related apps often process vast amounts of personal information from local and international users, making compliance with local legal standards both critical and complex. This study addresses this gap by assessing the compliance of tourism-related mobile apps with the PDPL and its implementation regulations, issued by the Saudi Data and Artificial Intelligence Authority (SDAIA). The assessment criteria are based on the requirements of the PDPL and cover key compliance dimensions, such as user consent, data minimization, user rights, security measures, breach notification, and cross-border data transfer. By focusing on the obligations of the Personal Data Protection Law (PDPL), this study provides a detailed understanding of the extent to which these applications comply with national data protection standards and highlights areas for improvement to better protect user rights.

II. METHODOLOGY

A comprehensive analytical framework was proposed that combines legal analysis, technical evaluation, and user experience assessment. The legal dimension is grounded in the provisions of the PDPL, with each app evaluated against relevant PDPL articles. The technical evaluation considers app permissions, data access practices, and update history. Additionally, the user experience perspective assesses the clarity and accessibility of privacy policies, usability, and language appropriateness. Each app was systematically assessed using a standardized rubric derived from the compliance checklist. To ensure the validity and reliability of the developed compliance rubric, two experts in the domain

reviewed the checklist. Feedback from these experts was incorporated to enhance the clarity and coverage of the items. Compliance assessment was carried out using quantitative approaches [19], following five steps as illustrated in Figure 1.

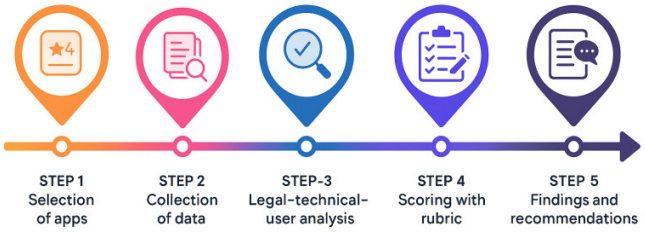

Fig. 1. Research method.

The first stage involved conducting a comprehensive review of the literature to identify and analyze previous studies related to personal data protection laws. In the second phase, the focus was exclusively on apps used during the Hajj and Umrah seasons in Saudi Arabia. A total of 66 apps were selected through a systematic search in Google Play and the Apple App Store. The inclusion criteria were: (i) relevance to Hajj or Umrah services (e.g., navigation, bookings, health, or religious guidance), and (ii) a minimum user rating of 4.0. Data collection was carried out between 20 September 2024 and 1 October 2024. The third stage examined the characteristics of the chosen apps, including app name, version, permissions requested, privacy policy availability, and last update. Descriptive statistical methods were employed to analyze the app characteristics and compliance levels, including frequency distributions, percentages, and cross-tabulations. In the fourth stage, each identified mobile application was systematically evaluated using a PDPL-aligned compliance framework, a structured rubric designed to assess adherence to the key principles (see Table I). The fifth and final stage involves the study findings and recommendations based on the analysis and evaluation carried out in the preceding stages. The documented dataset that includes details of all app features is available at [20].

TABLE I. PDPL-ALIGNED COMPLIANCE FRAMEWORK RUBRIC

Category	Compliance Criteria
A. User Data Rights	A1. Right to access data
	A2. Right to correct or update data
	A3. Right to delete data
	A4. Right to object to processing
	A5. Right to restrict processing
B. Data Protection Principles	B1. Lawfulness, fairness, and transparency
	B2. Purpose limitation
	B3. Data minimization
	B4. Storage limitation
	B5. Data accuracy
	B6. Data security
	B7. Accountability
C. Privacy Policy Compliance	C1. Data collection clause
	C2. Data processing clause
	C3. User rights clause
D. Breach and Cross-border Data	D1. Breach notification
	D2. Cross-border data transfer compliance

III. DATA ANALYSIS AND RESULTS

Table II illustrates that Google Play apps accounted for a higher percentage (81.8%) of the total compared to the Apple App Store (18.2%). Interestingly, the apps available on both platforms and developed by the same provider were only 6.6%. The study underscores a significant variance in the quantity of pilgrim apps available on Google Play compared to the Apple App Store. This contrast could be attributed to various factors, such as Android's broader market share, a potentially less rigorous review process for new apps, and lower developer fees associated with Google Play. Factors like this contribute to the disparity in app availability observed between the two stores.

TABLE II. PERCENTAGE OF APPS COLLECTED FROM STORES

	Store		
	Google Play	**App Store**	**Both**
Percentage	81.8%	18.2%	6.6%

A. Properties of the Selected Apps

1) Place of Origin

The analysis examined apps based on their place of origin, specifically examining the countries where pilgrim app developers are located. The data shown in Figure 2 offers intriguing observations regarding the geographical distribution of pilgrim app development. In particular, Saudi Arabia, the host of the holy cities of Makkah and Madinah, has the highest percentage (24.2%) of app development related to pilgrims. This finding aligns with the significant investments made by Saudi Arabia in technology and infrastructure to enhance pilgrim experience. The country's excellence in app development highlights its commitment to leveraging technology in the Hajj and Umrah sectors.

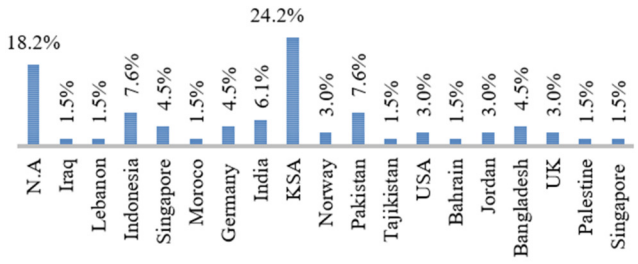

Fig. 2. Origin of app developers.

2) Recent Updates

This analysis shows a worrying picture of developer habits. As shown in Figure 3, only 30.3% of apps were updated in 2023 and 10.6% in 2022. A staggering 59.1% of apps went untouched for nearly a decade, from 2012 to 2021. In an era where technology evolves at a rapid pace, this lack of maintenance is alarming. Regular updates are not just about keeping up, they are critical for security and performance. When developers let updates slide, not only are they falling behind, but they are leaving doors wide open to risks. Developers should invest in timely updates before small oversights become major vulnerabilities.

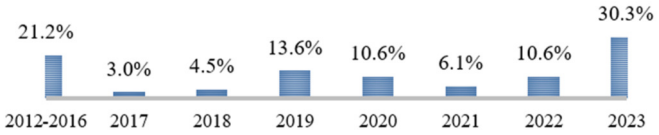

Fig. 3. Distribution of apps based on recent updates.

3) User Personal Data Requirements

The findings in Table III indicate that most of the surveyed apps do not require users to provide personal information, with only 6.1% requiring user registration. Registration, although it improves the user experience, raises privacy concerns as users share personal data. It is recommended that users review the app's privacy policy before registering. Additionally, 24.2% of apps allow voluntary input of personal data, such as name and date of birth. Furthermore, 22.7% advise enabling the Global Positioning System (GPS) for functionality, potentially raising privacy concerns. These results suggest that while direct collection of data such as names and phone numbers may not be a priority, indirect data collection through browsing behavior and cookies could still occur, highlighting potential misuse without user consent.

TABLE III. DISTRIBUTION OF APPS IN TERMS OF USER DATA REQUIREMENTS

Apps requirements	Rate
Registration is required to use the app	6.1%
Option to enter personal data	24.2%
Required/caution to enable GPS	22.7%

B. PDPL Compliance of the Selected Apps

1) User Personal Data Requirements

Figure 4 highlights concerns about the lack of compliance with users' data protection rights, including the right to object to processing, restrict usage, access, delete, correct or update, and process data. Compliance levels across these rights were notably low, ranging from 18.2% to 33.3%, reflecting a widespread disregard for user-centric privacy practices. This gap is worrying, as safeguarding personal data is a fundamental right essential for upholding privacy and other human rights. Several factors may explain this: limited awareness of PDPL obligations, lack of regulatory enforcement, or technical constraints in implementing rights-management mechanisms. The findings underscore the urgency for developers to prioritize data protection in mobile apps, especially in the tourism sector. Strengthening these measures requires collaboration between regulators, developers, and the broader ecosystem, aiming to raise awareness, provide technical guidance, and align development practices with PDPL principles.

2) Compliance with the User's Data Protection Principles

Figure 5 provides a comprehensive examination of how well developers comply with the principles of personal data protection in terms of lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, data security, accuracy, and accountability. The results demonstrate a serious lack of adherence to these principles, with 12.1% compliance rates in the area of responsibility being especially low. The overall range of compliance rates, which was 12.1% to 33.3%, indicated that data protection procedures need to be improved. This lack of adherence poses serious legal, ethical, and reputational risks. Effective data protection is not just a regulatory checkbox but a foundation for user trust. Lawfulness and fairness ensure respectful and rights-based data handling, and transparency empowers users to make informed choices. Similarly, minimizing and securely storing data for specific, time-bound purposes is crucial for privacy-respecting systems. These findings reveal a critical gap in integrating privacy-by-design principles during app development. Developers and organizations must embed PDPL principles early in design and update cycles and implement routine audits to ensure ongoing compliance.

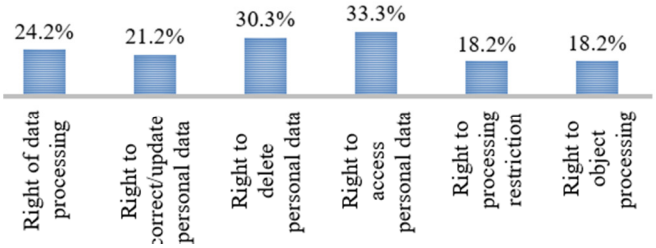

Fig. 4. App developers' compliance with users' data protection rights.

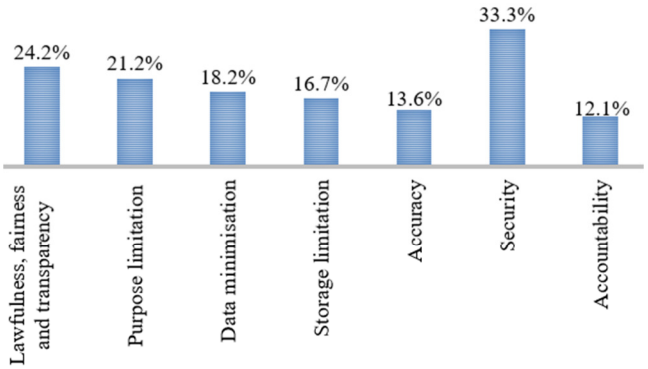

Fig. 5. App developers' compliance with users' data protection principles.

3) Compliance with Data Privacy

This study highlights the importance of the implementation of privacy policies in mobile applications to inform users about data collection and processing. Figure 6 reveals concerns about the compliance rates with privacy policies, ranging from 24.2% to 34.8% for data processing, collection, and rights clauses. These shortcomings underscore the urgent need for standardized policy templates and regulatory oversight to ensure clarity and completeness in privacy communications.

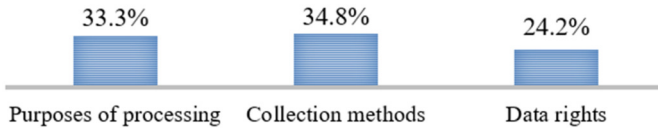

Fig. 6. App developers' compliance with data privacy.

4) Compliance with Extra-Territoriality Provisions and Breach Notifications

Saving sensitive data in the cloud can raise concerns about security theft and data breaches [21]. According to the PDPL, both local and foreign app developers must comply with regulations on resident data processing. However, the compliance rates among pilgrim app developers are concerning, with only 13.6% addressing compliance beyond the regional level (Figure 7). Developers are required to notify users of any data breach, helping mitigate risk. However, the low 4.5% compliance rate in breach notifications highlights a significant weakness in developers' data protection practices. Developers must implement clear breach notification protocols and be transparent about where and how user data are processed or transferred. Raising awareness about the extraterritorial scope of PDPL and building technical capabilities to monitor and respond to breaches is crucial to maintaining user trust and meeting legal obligations.

Fig. 7. App developers' compliance with extra-territoriality provisions and breach.

C. Best Apps in Terms of PDPL Compliance

This section highlights the top pilgrim-related apps that comply with the PDPL. Table IV presents a comprehensive overview of the essential features of apps, including the latest update, developer information, language used, and country of origin, along with their availability in the Google (G) or Apple (A) stores. In particular, these apps exceeded the 80% threshold on the compliance checklist, demonstrating their strong adherence to data protection regulations. The table illustrates a variety of app origins, including KSA, Germany, Singapore, and Norway, with English-language support predominating. In particular, recent updates for Nusuk and Saudia Umrah indicate ongoing app enhancements, signaling a focus on continuous development efforts compared to other apps.

TABLE IV. FEATURES OF MOBILE APPS THAT COMPLY WITH THE PDPL

App name	Last update	Developer	Languages	Country
Nusuk	01-Jul-23	Ministry of Haj & Umrah	Arabic, English	KSA
The Umrah Guide	26-May-20	Safar World	Multi-languages	Norway
Muslim 3D	03-Mar-19	Bigitec Studio	English, German	Germany
Saudia Umrah	04-Jun-23	Saudi Airlines	Arabic, English	KSA

Although prior studies on GDPR compliance (e.g., [9-13]) have identified systemic gaps in privacy practices, this analysis of 66 apps reveals even more severe shortcomings under the PDPL, particularly regarding compliance with extra-territoriality provisions and breach notification requirements, which stand at only 13.6% and 4.6%, respectively. These findings underscore the urgent need for PDPL-specific enforcement mechanisms to bridge the gap between legal frameworks and real-world implementation.

IV. CONCLUSION AND FUTURE WORK

The primary objective of this study was to assess the compliance of Hajj applications with Saudi personal data protection regulations, examining 66 apps and revealing a clear violation of users' basic rights across many articles of the PDPL. The compliance rate with the requirements to preserve users' data protection rights and the existence of personal data privacy policies ranged from 18.2% to 33.3%, indicating a significant deficiency in the fundamental rights of personal data. Additionally, the results indicate a lack of compliance with data protection requirements, with compliance rates ranging from 12.1% to 33.3%, raising concerns about data security, accountability, and transparency. Future research should aim to include a broader range of regulatory frameworks and industry sectors to provide a more comprehensive perspective on compliance and data protection practices. In addition, conducting an exhaustive survey, such as [22, 23], is needed to identify emerging trends and challenges.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the financial support provided by the Middle East University in Amman, Jordan, which covered the publication fees for this research article.

REFERENCES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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). Brusseles, Belgium: EU, 2016.

[2] "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | European Data Protection Board." https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

[3] "British Airways faces record £183m fine for data breach," Jul. 08, 2019. https://www.bbc.com/news/business-48905907.

[4] "Code of Virginia - Chapter 53. Consumer Data Protection Act." https://law.lis.virginia.gov/vacode/title59.1/chapter53/.

[5] "Data Protection Law," *Saudi Arabia*. https://sdaia.gov.sa/en/Research/Pages/DataProtection.aspx.

[6] "Home | Ministry of Tourism Saudi Arabia." https://mt.gov.sa/tic/dashboard/tourism-demand.

[7] "Forecast number of mobile users worldwide 2020-2025," *Statista*. https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010/.

[8] H. A. Aldhubaib, M. A. Abu-Hashem, and M. K. Shambour, "Standardization of Chargers for Portable Electronic Devices in the Saudi Market," *Journal of King Abdulaziz University-Engineering Sciences*, vol. 33, no. 2, pp. 67–81, 2023.

[9] M. Fan *et al.*, "An Empirical Evaluation of GDPR Compliance Violations in Android mHealth Apps," in *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*, Coimbra, Portugal, Oct. 2020, pp. 253–264, https://doi.org/10.1109/ISSRE5003.2020.00032.

[10] J. Muchagata and A. Ferreira, "Mobile Apps for People with Dementia: Are They Compliant with the General Data Protection Regulation (GDPR)?:," in *Proceedings of the 12th International Joint Conference on Biomedical Engineering Systems and Technologies*, Prague, Czech Republic, 2019, pp. 68–77, https://doi.org/10.5220/0007352200680077.

[11] N. Momen, M. Hatamian, and L. Fritsch, "Did App Privacy Improve After the GDPR?," *IEEE Security & Privacy*, vol. 17, no. 6, pp. 10–20, Nov. 2019, https://doi.org/10.1109/MSEC.2019.2938445.

[12] D. S. Guamán, J. M. Del Alamo, and J. C. Caiza, "GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Apps," *IEEE Access*, vol. 9, pp. 15961–15982, 2021, https://doi.org/10.1109/ACCESS.2021.3053130.

[13] Q. Jia, L. Zhou, H. Li, R. Yang, S. Du, and H. Zhu, "Who Leaks My Privacy: Towards Automatic and Association Detection with GDPR Compliance," in *Wireless Algorithms, Systems, and Applications*, 2019, pp. 137–148, https://doi.org/10.1007/978-3-030-23597-0_11.

[14] S. E. Polykalas and G. N. Prezerakos, "When the mobile app is free, the product is your personal data," *Digital Policy, Regulation and Governance*, vol. 21, no. 2, pp. 89–101, Jan. 2019, https://doi.org/10.1108/DPRG-11-2018-0068.

[15] F. H. Shezan, Y. Lao, M. Peng, X. Wang, M. Sun, and P. Li, "NL2GDPR: Automatically Develop GDPR Compliant Android Application Features from Natural Language," in *2022 IEEE Conference on Communications and Network Security (CNS)*, Austin, TX, USA, Oct. 2022, pp. 1–9, https://doi.org/10.1109/CNS56114.2022.10273858.

[16] M. Hatamian, "Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers," *IEEE Access*, vol. 8, pp. 35429–35445, 2020, https://doi.org/10.1109/ACCESS.2020.2974911.

[17] K. Bongard-Blanchy, J. L. Sterckx, A. Rossi, V. Distler, S. Rivas, and V. Koenig, "An (Un)Necessary Evil - Users' (Un)Certainty about Smartphone App Permissions and Implications for Privacy Engineering," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Genoa, Italy, Jun. 2022, pp. 01–08, https://doi.org/10.1109/EuroSPW55150.2022.00023.

[18] M. Farhadi, G. Pierre, and D. Miorandi, "Towards automated privacy compliance checking of applications in Cloud and Fog environments," in *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Rome, Italy, Aug. 2021, pp. 11–18, https://doi.org/10.1109/FiCloud49777.2021.00010.

[19] M. K. Y. Shambour, "Assessing the Usability of Hajj and Umrah Websites," in *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, Jul. 2021, pp. 876–881, https://doi.org/10.1109/ICIT52682.2021.9491780.

[20] "Apps Data." Sharepoint, [Online]. Available: https://stumeuedu-my.sharepoint.com/:x:/g/personal/m_shambour_meu_edu_jo/EZhW0Cqs-05HjLzudyUe0K0BeVtMKBRvSSAHd2kAvT8UzA?rtime=DS-lVQKk3Ug.

[21] A. I. Abueid, "Big Data and Cloud Computing Opportunities and Application Areas," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14509–14516, Jun. 2024, https://doi.org/10.48084/etasr.7339.

[22] A. Raghuvanshi, U. K. Singh, and C. Joshi, "A Review of Various Security and Privacy Innovations for IoT Applications in Healthcare," in *Advanced Healthcare Systems*, John Wiley & Sons, 2022, pp. 43–58.

[23] S. Almuaythir, A. K. Singh, M. Alhusban, and A. O. Daoud, "Robotics technology: catalyst for sustainable development—impact on innovation, healthcare, inequality, and economic growth," *Discover Sustainability*, vol. 5, no. 1, Dec. 2024, Art. no. 486, https://doi.org/10.1007/s43621-024-00744-y.