Management & Marketing
Volume 20 Issue 3 · pp. 28–47 · DOI: 10.2478/mmcks-2025-0015

sciendo

Management & Marketing

Privacy and security in mobile technology: A bibliometric analysis for marketing strategies

Research Article

Hasna Koubaa El Euch[1], Foued Ben Said[2], Rim Jallouli[3]*

[1] *University of Manouba, ISCAE, LIGUE Laboratory, Manouba, Tunisia*
[2] *University of Manouba, ESCT, MOCFINE Laboratory, Manouba, Tunisia*
[3] *University of Manouba, ESEN, LIGUE Laboratory, Manouba, Tunisia*

Received 03 July 2025; Accepted 09 September 2025

Abstract: Privacy and security have become critical issues within the realm of mobile technology (MT), drawing increasing attention from both academics and business community. In response, scholars across computer science, engineering, management, and marketing have increasingly addressed these concerns, recognizing their significance in theory and practice. However, the broad spectrum and the multidisciplinary nature of publications within this topic have led to a fragmented body of literature that needs a cohesive structure. This study aims to unify the existing knowledge by offering a comprehensive overview of academic contributions at the intersection of MT, privacy, and security. Specifically, it examines how privacy and security considerations influence segmentation, targeting, and positioning strategies. A bibliometric analysis was performed using Bibliometrix software along with Biblioshiny and PlantUML tools, applying both performance analysis and science mapping techniques. One thousand fifty-seven documents were sourced and analyzed from the Web of Science database, covering the years 1996–2023. Key findings include the identification of an emerging cluster on "machine learning" and a niche cluster labeled "sensors." The results underscore significant gaps in the existing literature, paving the way for future research to address ongoing challenges and explore new opportunities in MT and marketing strategies related to privacy and security.

Keywords: *Bibliometric analysis* • *Marketing strategies* • *Mobile technology* • *Privacy* • *Security*

1. Introduction

The rapid growth of mobile technology (MT), along with rising concerns related to privacy and security, has drawn increasing attention from both academics and business community. This interest spans multiple disciplines, including computer science, engineering, data science, cybersecurity, management, and marketing. Over the past decade, numerous studies have addressed privacy and security issues in the field of MT, covering related constructs such as trust, confidentiality, anonymity, identity, and authentication.

In software engineering, researchers such as Ebrahimi et al. (2021) and Buck and Burster (2017) have investigated mobile application privacy, focusing on topics like data leakage detection and user concerns about app-related privacy. In the field of blockchain, Dhar and Bose (2020) developed a comprehensive mobile Internet of Things (IoT) security framework that uses a risk-scoring methodology to manage IoT security risks. Likewise, in the emerging field of 6G network edge technologies, Mao et al. (2023) introduced novel approaches to mitigate privacy and security threats inherent to the evolving 6G ecosystem.

In marketing, prior research shows the growing role of MT in different contexts such as mobile commerce (Thakur & Srivastava, 2013), mobile marketing (Narang & Shankar, 2019; Thangavel & Chandra, 2023), mobile applications (Sakas & Giannakopoulos, 2021), and mobile advertising (Bakar & Bidin, 2014; Gao & Zang, 2016; Serrano-Malebran et al., 2023). As a result, privacy and security concerns have become central to developing effective marketing strategies. A recent bibliometric study by Koubaa et al. (2024) identified trust and privacy as core elements in mobile commerce and marketing. From a practical perspective, marketers increasingly

* *E-mail: rimjallouli@esen.tn*

struggle to leverage MT while addressing consumer concerns related to privacy, trust, personalization, and data security (Hentati & Jallouli, 2024).

Within this context, the present study explores how MT can be strategically utilized to improve marketing practices while addressing privacy and security challenges. It aims to synthesize the existing body of knowledge and underscore the role of MT in shaping marketing strategies, particularly in relation to segmentation, targeting, and positioning (STP). Although a substantial body of literature exists, it remains fragmented due to the multidisciplinary nature of the field and rapidly evolving technological trends.

To address this gap, we performed a bibliometric analysis using Bibliometrix software and complementary tools such as Biblioshiny and PlantUML. Bibliometric methodology has proven rigorous for exploring and analyzing large volumes of scientific data (Donthu et al., 2021), effective in revealing the structure and dynamics of research fields (Ozturk, 2021), particularly in business strategy and marketing (Hu et al., 2019).

This study addresses the following Research Questions (RQs):

- **RQ1**: What is the current state of research on MT related to privacy and security within marketing strategies?
- **RQ2**: What are the key research gaps and future directions regarding the role of MT in addressing privacy and security concerns in marketing contexts?

The remainder of this article is organized as follows: Section 2 presents a literature review, beginning with privacy and security issues in MT and then exploring marketing responses to these concerns. Section 3 outlines the bibliometric approach used, including performance analysis. Section 4 provides the findings of the science mapping. Finally, Section 5 interprets the results, highlights limitations, and offers recommendations for future research at the intersection of MT, privacy/security, and marketing.

2. Related literature

This section gives a closer examination of related works contributed in MT focusing on privacy and security concerns in association with marketing strategies. Two subsections are presented to lay an overview of the literature in this research. The first one provides insights into the concept of MT focusing on privacy and security concerns. The second sub-section identifies marketing strategies, mainly STP strategies related to MT, privacy, and security concerns.

2.1 MT highlighting privacy and security concerns

"The significance of research in the realms of privacy and security cannot be overstated, as these areas necessitate continuous advancements and innovative solutions" (Lakshmi & Kumar, 2017). In the field of Software Engineering, Ebrahimi et al. (2021) conducted a study on mobile application privacy between 2008 and 2018. Their findings revealed that most current research emphasizes the creation of tools for detecting privacy leaks, while there remains a notable scarcity of studies addressing key aspects such as "privacy requirements," "privacy policies," and "user perspectives."

Dhar and Bose (2020) examined the security challenges inherent in the deployment of IoT devices, including mobile IoT, and proposed an integrated security framework that leverages Zero Trust principles and blockchain technology to enhance identity verification and access control within IoT ecosystems. Various cybersecurity approaches have also been developed to safeguard autonomous vehicles from cyberattacks. Poddar et al. (2024) explored the application of machine learning (ML) and deep learning methods to bolster defense mechanisms in autonomous vehicles, which rely on easily manipulated technologies such as cameras, ultrasonic sensors, and infrared sensors. Similarly, Wang et al. (2021) introduced a model-based framework using multi-sensor data to detect and isolate sensor-based attacks within transportation systems.

Zhang et al. (2022) addressed data privacy and security concerns in agricultural IoT by incorporating cryptographic and blockchain solutions to ensure secure management of agricultural data. Mao et al. (2023) investigated 6G edge network technologies, emphasizing their potential for advanced service delivery while identifying critical unresolved security issues.

A comprehensive reading of the literature suggests that privacy and security concerns are multifaceted and continuously evolving across various technological ecosystems, including mobile applications, IoT devices, autonomous vehicles, and next-generation networks. Despite notable technological advancements, much of the existing work approaches these issues from a predominantly technical perspective, often overlooking critical dimensions such as user expectations, regulatory frameworks, and the strategic implications for marketing. Foundational elements like privacy policies and the alignment of security measures with trust-building strategies remain underexplored. Additionally, while innovations span diverse sectors, limited cross-sectoral synthesis hampers a holistic understanding of how such technologies can be deployed securely and responsibly in consumer-facing contexts. By integrating insights from these disparate domains and linking them to marketing-oriented concerns, this study puts forward an interdisciplinary framework that identifies concrete directions for future research and meaningful guidance for practitioners.

2.2 Marketing strategy related to MT with privacy and security concerns

Marketers face significant challenges in adopting technological innovations while addressing key concerns such as consumer privacy, data security, personalization, loyalty, confidentiality, and the detection of data breaches.

Varnali and Toker (2010) emphasized the importance of ensuring mobile user privacy and security. Within consumer policy, mobile marketing raises critical issues due to the unique capabilities of mobile communication technologies, which allow for the identification of individual users. This characteristic introduces considerable risks to the privacy and security of personal information – risks that are further intensified by the increased adoption of mobile marketing among younger consumers (Purwanto et al., 2020).

Sinha et al. (2019) investigated privacy concerns and provided insights into enhancing both security mechanisms and user experience. Similarly, Ullah et al. (2023) analyzed privacy risks associated with targeted mobile advertising and proposed solutions to mitigate these concerns.

This body of research highlights the need for future work focused on the development of user-centered privacy protection tools that promote transparency in data usage and empower individuals to safeguard their personal information in mobile advertising contexts.

Rafieian and Yoganarasimhan (2021) investigated the relationship between mobile in-app advertising, regarded as the leading form of digital marketing, and targeting efficiency associated with privacy concerns and economic results. Considering social media marketing as a segmentation tool, Serrano-Malebran et al. (2023) explore relationship between consumer classifications and variables such as privacy concerns, trust and age. In the field of mobile social networks, Lakshmi and Kumar (2017) consider the privacy protection and security as critical issues requiring constant updates and solution development. The convergence of these studies reveals a growing strategic imperative for marketers to integrate privacy and security considerations into the design of MT and personalized marketing tools. The literature underscores not only the operational risks associated with data misuse and breaches, but also the reputational and trust-related consequences that directly influence consumer engagement and brand loyalty. While multiple technological and behavioral insights are offered, there remains a gap in cohesive frameworks that align privacy-by-design principles with STP strategies. Furthermore, few studies provide actionable models that reconcile personalization with ethical data practices across platforms and demographics. This fragmented landscape suggests a need for more integrative approaches to ensure that MT contribute meaningfully and responsibly to long-term strategic objectives.

In this regard, the study aims to synthesize core insights from the existing body of literature and to highlight the role of MT in shaping marketing strategies, particularly through the lens of STP.

3. Methodology

This study meticulously explores the evolution of research on MT, privacy and security related to marketing strategies by conducting a comprehensive bibliometric analysis, utilizing data from the WoS, recognized for its reliable and comprehensive metadata (Pranckutė, 2021; Zhu & Liu, 2020). According to AlRyalat et al. (2019), the WoS database has several distinctive advantages that make it a reference database for bibliometric research. First, its universal disciplinary coverage encompasses all academic disciplines. Second, with historical coverage dating back to 1900, WoS allows in-depth longitudinal bibliometric analyses. Third, its advanced features, in particular the search, distinguish this database for data associated with publications, and sophisticated tools for producing figures. The study analyzed 1,057 documents covering the period from 1996 to 2023. The analysis employed a multifaceted approach, examining the temporal distribution of publications, assessing key contributors and influential works to chart the field's historical trajectory, and creating a thematic map through a science mapping technique based on keyword co-occurrences. This thematic map unveiled basic themes, core and niche research areas, emerging trends, and potential gaps within the literature.

3.1 Process for document selection

The process of selecting documents from the WoS database is presented in Table A1.

This search query aims to identify articles in English that discuss the intersection of marketing strategies with MT, privacy and security concerns. It combines three separate searches: the first focuses on marketing strategies (including STP strategies), the second explores MT (including ML, IoT, blockchain, recommender systems, and tracking technologies), and the third examines privacy and security. The final search combines these three, filtering for articles only, ensuring the results focus on scholarly research.

3.2 Bibliometric tools

In this comprehensive bibliometric analysis, the study strives to map the literature's temporal evolution and delineate its developmental phases. Furthermore, it identifies and evaluates the most influential journals, pinpointing those that have significantly shaped the discourse in this domain. This research will highlight the most impactful authors, recognizing their contributions to advancing knowledge in the field. Additionally, this analysis uncovers the most cited documents and references, thereby illuminating the seminal works that have laid the foundation for current research and that continue to drive scholarly discussions.

This study employed a bibliometric analysis approach supported by multiple tools. The primary analysis was conducted using Bibliometrix, an R package integrated into R version 4.4.0 and executed within the RStudio environment (Aria & Cuccurullo, 2017). To facilitate accessibility and enhance the visualization of results, the study utilized Biblioshiny, a web-based interface that enables interactive, user-friendly bibliometric analysis and graphical output. For concept maps creation, the study made use of PlantUML (https://plantuml.com/en/), an online diagramming tool. PlantUML allows for the generation of thematic concept maps from simple text-based inputs, offering a clear and visually appealing representation of the study's conceptual framework.

3.3 Database characteristics

Table A2 provides a snapshot of the research landscape surrounding MT, privacy, and security, highlighting the field's rapid growth and international collaboration.

The dataset spans 28 years, from 1996 to 2023, and includes over 1,000 documents from 502 sources. The 21.79% annual growth rate indicates a significant increase in research activity. The average of 18.22 citations per document echoes high impact and relevance of the research within the field. The high percentage of international coauthorships (33.77%) evinces a global collaboration in tackling these complex issues. This suggests an expanding field with considerable international interest.

3.4 Temporal publication evolution

Figure 1 depicts the annual evolution of publications on MT, privacy, and security for marketing strategies from 1996 to 2023, revealing a noteworthy trend over time. Initially, from 1996 to 2008, the number of articles published each year was minimal, indicating limited academic interest in this intersection. However, a gradual increase starting in 2009 marks the onset of a growing recognition of privacy issues in MT. This period of steady growth, which continued until 2018, reflects a more sustained academic focus. A dramatic surge in publications is evident from 2019 onwards, with the number of articles exceeding 200 annually in 2021 and 2022, showcasing an intensified focus, likely driven by advancements in MT, elevated device usage, and rising privacy concerns. Although 2023 reveals a slight decrease, the publication numbers remain high, suggesting a stabilization or a possible shift in research focus.

Scientific production in the field of MT, in relation to privacy, security, and marketing strategies, has grown remarkably since 2017, stimulated by the emergence and convergence of innovative technological concepts such as wireless sensor networks (WSN), IoT, ML, deep learning, and blockchain technology.

3.5 Journals performance

Table 1 presents key indicators of journal influence and impact within the research area of MT, privacy, and security. These indicators, including h-index (Hirsch, 2005), g-index, m-index, total citations (TC), number of publications (NP), and the starting year of publication (PY_start), allow researchers to assess the relative influence of these journals within the field.

The journals *IEEE Access*, *IEEE Internet of Things Journal*, and *Sensors* are currently leading the field in terms of impact and research output. Their high h-index, g-index, and total citations demonstrate their significant contributions to the field. Interestingly, the table also highlights the emergence of newer journals like *IEEE Communications Surveys & Tutorials* and *Future Generation Computer Systems*, which are quickly gaining traction. This implies a dynamic research landscape where established journals are complemented by rising publications shaping a diverse and evolving research environment.

IEEE Access journal explores the crucial intersection of MT, privacy, and security in the context of IoT, 5G, and Industry 5.0. It covers advanced topics like blockchain, federated learning, and ML, focusing on their applications in enhancing mobile privacy and security. By investigating

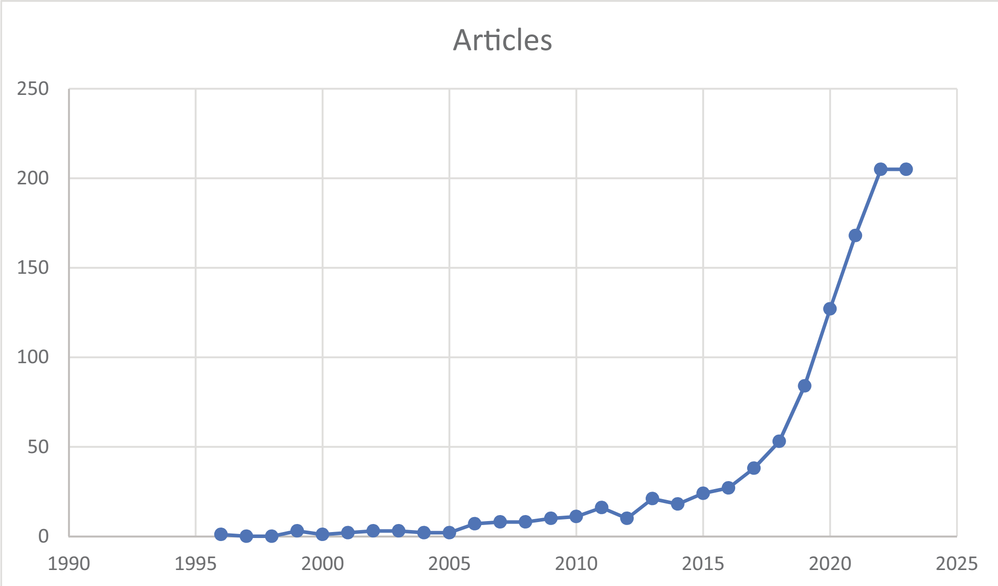

Figure 1. Temporal publication evolution.

Source: Authors' own research.

practical applications in areas like smart healthcare and social distancing, the journal demonstrates the relevance of these technologies to marketing and consumer behavior.

3.6 Authors' performance

Table 2 presents a detailed analysis of the scholarly performance metrics for three authors: Kim-Kwang Raymond Choo, Enrico Cambiaso, and Ivan Vaccari. Each author's performance is quantified using several indices: the h-index, g-index, m-index, total citations (TC), number of publications (NP), and the year they started publishing (PY_start).

Kim-Kwang Raymond Choo is a leading researcher in the field of cybersecurity, particularly focusing on the privacy and security issues posed by emerging technologies like IoT and autonomous vehicles. His research explores both theoretical and practical aspects of these challenges. He has developed solutions for cross-domain authentication in drone networks using blockchain, proposed security methodologies for self-driving vehicles, and conducted large-scale analyses of IoT vulnerabilities.

Journal	h_index	g_index*	m_index**	TC	NP	PY_start
IEEE Access	24	45	2.667	2,178	83	2016
IEEE Internet of Things Journal	15	27	2.143	887	27	2018
Sensors	15	24	1.25	702	51	2013
IEEE Communications Surveys & Tutorials	10	10	1.25	1,736	10	2017
Future Generation Computer Systems	9	12	1.125	339	12	2017
IEEE Sensors Journal	9	17	0.9	489	17	2015
Computers & Security	8	11	1.143	226	11	2018
IEEE Transactions on Intelligent Transportation Systems	8	15	0.444	380	15	2007
Wireless Personal Communications	7	13	0.318	198	17	2003

*g-index: calculated based on the distribution of citations received by a given researcher's publications (Egghe, 2006).
**m-index: calculated by dividing h-index value by number of years since the author is active (Srivastava et al., 2021).
Table 1. Most impactful journals with h-index equal or upper than seven.

Source: Authors' own research.

Author	h_index	g_index	m_index	TC	NP	PY_start
Kim-Kwang Raymond Choo	5	5	0.833	218	5	2019
Enrico Cambiaso	4	4	0.5	69	4	2017
Ivan Vaccari	4	4	0.5	69	4	2017

Table 2. Most impactful authors with h-index up or equal to four.

Source: Authors' own research.

Enrico Cambiaso is a researcher specializing in IoT security, focusing on vulnerabilities in protocols like message queuing telemetry transport (MQTT), and developing novel attack methods. He has demonstrated the effectiveness of a low-rate Denial of Service (DoS) attack, SlowITe, which exploits a weakness in MQTT to disrupt service. His research highlights the importance of understanding and mitigating security risks in IoT environments, particularly for critical infrastructure and sensitive data transmission.

Ivan Vaccari is focusing on security vulnerabilities in IoT networks, precisely targeting the MQTT protocol. He has identified weaknesses in MQTT that allow clients to manipulate server behavior and has developed innovative low-rate DoS attacks, like SlowITe and SlowTT that exploit these weaknesses. His research sheds light on the need for robust security measures in IoT environments to mitigate these vulnerabilities and ensure reliable operation.

3.7 Top most cited papers

Table 3 presents a comprehensive overview of the most impactful documents, offering an essential foundation for a bibliometric analysis.

These most cited studies explore various aspects of privacy and security in emerging technologies, from wireless networks to the IoT and even medical applications. Capkun and Hubaux (2006) address vulnerabilities in positioning techniques to spoofing attacks, proposing a mechanism called "verifiable multilateration" to secure location data in wireless networks. Chaabouni et al. (2019) delve into the security challenges of IoT networks, analyzing existing intrusion detection systems and advocating for ML techniques to enhance detection capabilities. Kalnis et al. (2007) tackle the issue of privacy in location-based services, proposing methods for anonymizing spatial queries while preserving result accuracy. Song et al. (2020) introduce a framework that leverages blockchain and deep learning to improve vehicular positioning accuracy and security in the Internet of Vehicles. Li et al. (2020) suggest a blockchain-based system for secure and efficient global positioning system (GPS) error sharing among vehicles, contributing to more accurate positioning in autonomous driving. Finally, Kumar et al. (2021) explore the use of blockchain and federated learning in medical applications, presenting a framework for collaborative training of deep learning models for COVID-19 detection and ensuring data privacy.

Paper	Title	Year	Local citations	Global citations
Capkun and Hubaux (2006)	Secure positioning in wireless networks	2006	7	191
Chaabouni et al. (2019)	Network Intrusion Detection for IoT Security Based on Learning Techniques	2019	7	379
Kalnis et al. (2007)	Preventing Location-Based Identity Inference in Anonymous Spatial Queries	2007	6	358
Song et al. (2020)	Blockchain-Enabled Internet of Vehicles with Cooperative Positioning: A Deep Neural Network Approach	2020	5	51
Li et al. (2021)	Vehicle Position Correction: A Vehicular Blockchain Networks-Based GPS Error Sharing Framework	2021	5	62
Kumar et al., (2021)	Blockchain-Federated-Learning and Deep Learning Models for COVID-19 Detection Using CT Imaging	2021	5	180

Table 3. Most cited papers.

Source: Authors' own research.

4. Science mapping analysis

Science mapping analysis provides a comprehensive bibliometric approach to visualizing and analyzing the intellectual structure and knowledge dynamics within a specific research domain. This section comprises two key analytical components: references co-citation network analysis and thematic map exploration.

4.1 References co-citation network

The co-citation network analysis in this study employs a visual representation to illustrate the interconnectedness of different research articles based on their shared citations. This network highlights which papers are frequently cited together, indicating their potential conceptual or methodological connections. This analysis helps identify clusters of research themes and understand how knowledge within a field evolves (Zhang et al., 2021). Figure 2 illustrates the references co-citation network. A threshold of seven citations has been used so that only references that have been cited at least seven times in the study corpus will be represented in the network map. Out of 4,747 references cited, only 115 reach this minimum threshold, which makes it possible to filter and focus only on the most influential and frequently referenced works in the field. It identifies three distinct clusters, represented in red, green, and blue, respectively, titled IoT devices, privacy-preserving techniques, and neural network architectures. Together, these clusters offer a comprehensive view of the technological innovations, ethical imperatives, and strategic opportunities that drive the evolution of MT marketing, ensuring that practices remain both cutting-edge and responsible.

4.2 IoT devices (red cluster)

This cluster provides a valuable overview of the research surrounding the proliferation of IoT devices. It highlights the rapid growth of this technology and its potential to revolutionize various industries and aspects of our lives. The studies by Al-Fuqaha et al. (2015) provide a foundational overview of IoT technologies and applications, setting the stage for subsequent research. Raza et al. (2013) address early security concerns by introducing SVELTE, an intrusion detection system for resource-constrained IoT devices. As threats evolved, Meidan et al. (2018) proposed N-BaIoT, an advanced network-based anomaly detection method using deep autoencoders to identify compromised IoT devices. To support ongoing research and development, Koroniotis et al. (2019) developed the Bot-IoT dataset, incorporating legitimate and simulated IoT network traffic with various attack types.

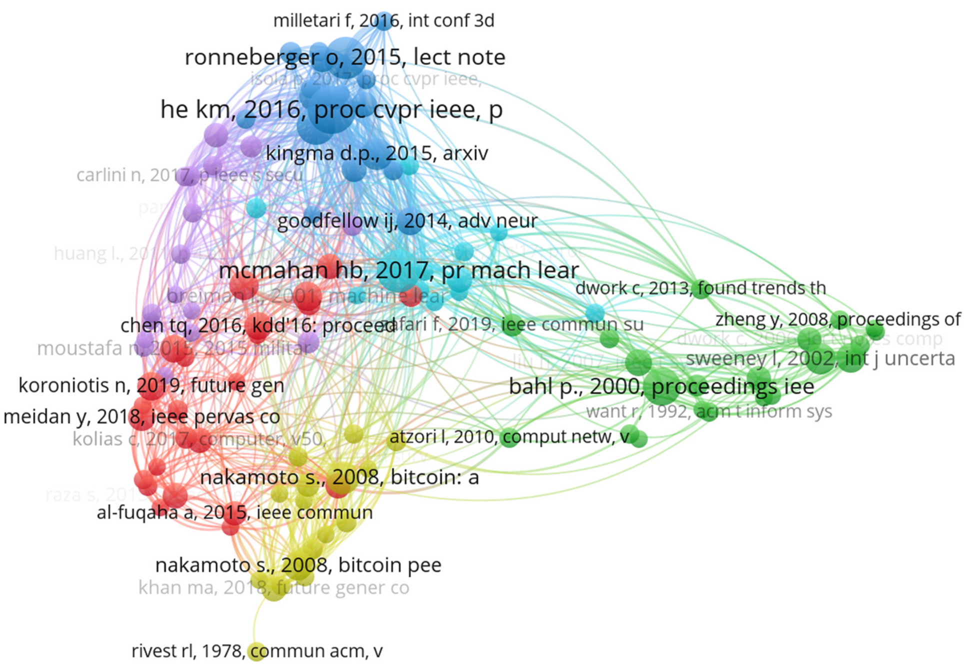

Figure 2. References co-citation network.

Source: Authors' own research.

4.3 Privacy-preserving techniques (green cluster)

This cluster encompasses studies that showcase significant advancements in privacy-preserving techniques across diverse data types and applications. Dwork et al. (2006) introduced the concept of differential privacy, proposing a method to add calibrated noise to statistical database queries to preserve individual privacy while maintaining data utility. Gruteser and Grunwald (2003) developed a middleware architecture for location-based services that adjusts the spatial and temporal resolution of location data to meet anonymity constraints. Sweeney (2002) presented the *k*-anonymity model for protecting privacy in released datasets, ensuring that each individual's information is indistinguishable from at least $k-1$ others. Finally, Beresford and Stajano (2004) introduced the concept of mix zones for location privacy in pervasive computing, along with metrics for assessing user anonymity in frequently changing pseudonyms.

4.4 Neural network architectures (blue cluster)

The studies in this cluster highlight significant advancements in neural network architectures and datasets, driving progress in the field of computer vision. Krizhevsky et al. (2017) introduced AlexNet, a breakthrough convolutional neural network that significantly improved ImageNet classification. Moreover, He et al. (2016) presented ResNet, introducing residual learning for training very deep networks. Simonyan and Zisserman (2014) proposed VGGNet, demonstrating the importance of network depth with small convolutional filters. Finally, Deng et al. (2009) introduced ImageNet, a large-scale image database that became crucial for training and evaluating deep learning models.

4.5 Thematic map

The thematic map in bibliometric analysis organizes research themes based on centrality (importance) and density (development level) (Callon et al., 1991; Cobo et al., 2011; Meyer et al., 2023). This visualization helps researchers identify research gaps, emerging trends, and the overall landscape of a field, highlighting potential areas for investigation. Figure 3 presents the thematic map for this study. The parameters used to construct this thematic map include a selection of the 250 most frequent words, with a minimum threshold of five occurrences per thousand documents for the formation of clusters. Each cluster is limited to a maximum of three labels with a size of 0.3 to optimize readability. The Louvain algorithm has been applied for the detection of thematic communities, while a community repulsion parameter of 0.1 ensures an appropriate visual separation between the different groups of concepts on the map.

The conceptual maps in this section are derived from keyword clusters, with their visual representations

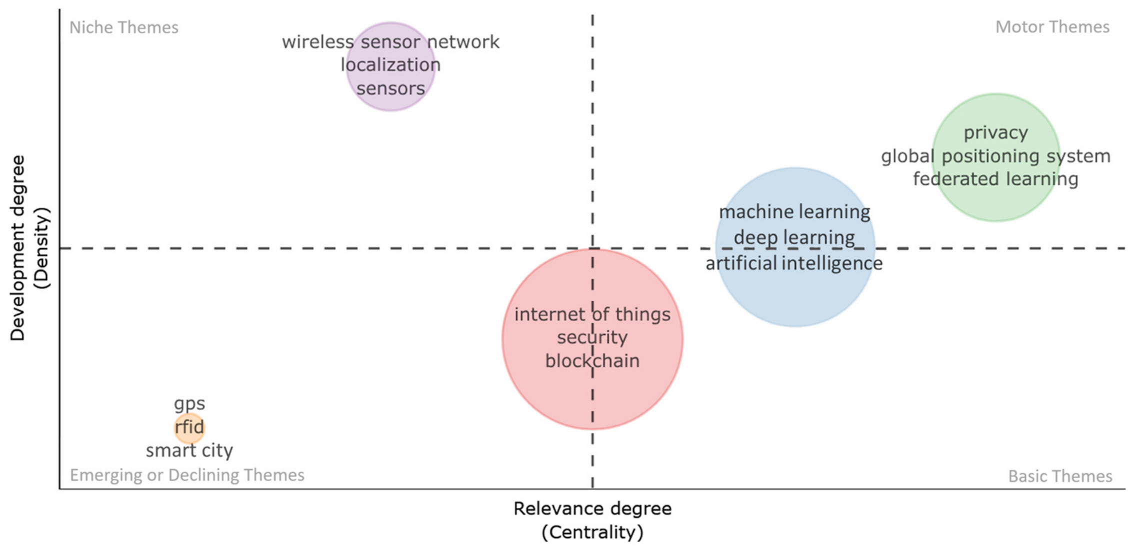

Figure 3. Thematic map.

Source: Authors' own research.

generated using the PlantUML website. These maps are constructed based on the frequency and co-occurrence of keywords within the literature.

4.6 ML cluster: Evolving from basic to motor themes

This cluster examines the transformative impact of AI and ML on marketing practices, focusing on customer segmentation, predictive analytics, and customer behavior analysis. The studies reveal how AI is being used to optimize audience targeting by going beyond traditional optimal distinctiveness and tailoring strategies to different revenue models (Majzoubi & Zhao, 2023; Van Angeren et al., 2022). Predictive models are being implemented to remedy crucial challenges like food security, crop yield estimation, and financial risk assessment (Gambetti et al., 2022). AI is additionally empowering personalized recommendations and driving strategic decision-making in areas like advertising and IoT adoption (Shi et al., 2022). However, the review highlights the need to address privacy concerns, ensure explainability, and foster continuous learning to promote accountable and effective AI deployment in the ever-evolving marketing landscape.

Clark et al. (2023) address the issue of "user disambiguation," which aims to identify individual viewership within multi-person households. Their ML approach provides accurate insights for television ad targeting and audience analysis, a valuable tool for marketers in the entertainment industry. Additionally, Peng and Xin (2019) propose a social trust and preference segmentation-based recommendation algorithm to improve personalized suggestions. By incorporating trust relationships and preference domains, this algorithm enhances the effectiveness of recommendation systems in e-commerce platforms. Furthermore, an AI-based real-time positioning advertising system leveraging 5G base station data enhances the efficiency of audience targeting and personalized advertisement delivery, unlocking new opportunities for location-based marketing strategies (Cheng & Wang, 2021).

4.7 Privacy cluster: Established motor themes

This cluster examines the complex relationship between privacy technologies, data handling, learning and modelling, positioning and navigation, advanced technologies, and finally ethics and safety.

The explosive growth of data, particularly location data from GPS-enabled devices, offers unprecedented opportunities for personalized marketing. AI-powered algorithms perform accurate analyses of these data to predict consumer behavior, segment customers, and tailor marketing messages (Benslama & Jallouli, 2020, 2022, 2024; De Sousa et al., 2023). However, this level of personalization comes at a cost: consumer privacy. The studies reviewed highlight several key concerns and trends related to positioning and navigation, advanced technologies, ethical and safety-privacy technologies, data handling learning and modelling. Results show, for example, that location data from GPS-enabled devices, such as smartphones, are incredibly valuable for understanding consumer behavior and creating highly personalized marketing campaigns (Nanni et al., 2016; Stachl et al., 2020). However, location data are also highly sensitive and can reveal a vast amount of personal information (Michael & Clarke, 2013; Simpson, 2014). Consequently, there is an urgent need for robust privacy-preserving techniques to anonymize or obfuscate location data before it is used for marketing purposes (Kalnis et al., 2007; Peng et al., 2014). Studies demonstrate that even anonymized location data can be re-identified, requiring advanced privacy-enhancing solutions (Hoh et al., 2010).

As a result, consumers are increasingly aware of and concerned about the collection and use of their personal data, particularly location data (Banerjee, 2019; Milne & Bahl, 2010). This awareness is leading to a demand for more transparency and control over data usage (Yang & Kels, 2016). Public trust in data service providers varies depending on their familiarity and the type of data collected (Banerjee, 2019). Therefore, there is an expanding need for ethical considerations and regulatory frameworks to address these concerns (Milne & Bahl, 2010; Teodorescu et al. 2025; Yang & Kels, 2016). Federated learning is emerging as a promising solution for balancing the needs for personalization and privacy (Cheng et al., 2022; Huo et al., 2023). Several studies showcase the potential of federated learning for privacy-preserving marketing applications, including user profile construction (Huo et al., 2023) and travel time prediction (Zhu et al., 2021).

4.8 Sensors cluster: Specialized niche themes

The niche cluster of sensors identifies a critical research gap in the literature concerning the integration of sensors, global navigation satellite system, and various data security techniques within emerging technologies such as smart cities and cyber-physical systems. Zakroum et al. (2022) and Orouji and Mosavi (2020) demonstrate the vulnerabilities of network telescopes and IoT devices to attacks, emphasizing the need for robust security measures. Simultaneously, research on privacy-preserving techniques, such as differential privacy and anonymization, explored by Liu et al. (2023), remains critical to protecting user data in increasingly sensor-rich environments. Researchers like Kong et al. (2022) and Wu (2022) are tackling these challenges by incorporating federated learning and blockchain technologies within 6G networks and intelligent transportation systems. However, the integration of sensor phenomena and characterization, along with the complex dynamics of cyber-physical systems, requires further investigation to ensure responsible and secure deployment of these advanced technologies.

4.9 Security cluster: Advancing from emerging toward motor themes

Results illustrate the multifaceted nature of security, structured around six main dimensions: Data Security, Enabling Technologies, Marketing Security, Trust and Reputation, MT Security, and Network Security. Data Security encompasses privacy measures, Encryption, and Cybersecurity to protect sensitive information. Enabling Technologies include blockchain, 5G, cyber-security, and authentication to enhance security across various platforms. Results show that Marketing security was studied mainly concerning the concept of cyber-security. The branch of Trust and reputation focuses on the authentication concerns. MT Security focuses on IoT, device protection, and GPS security. Finally, Network Security involves intrusion and anomaly detection to safeguard against unauthorized access and cyber-attacks.

5. Discussion

Analysis generated from the science mapping highlights how MT is increasingly intertwined with concerns of privacy and security. These concerns are strategic enablers of trust in marketing. Security forms a foundational layer, encompassing not only the protection of network and data but also the trust that facilitates consumer acceptance of data-driven marketing. Privacy, in turn, emerges as core theme that links technical safeguards with consumer-facing issues such as transparency, consent, and the ethical use of data.

The co-citation network analysis (Figure 2) identified three clusters relevant to MT marketing: (1) IoT devices, which collect real-time, context-based consumer data; (2) privacy-preserving techniques, which ensure the responsible and ethical use of such data; and (3) neural network architectures, which generate deeper insights to enhance STP.

IoT enables dynamic segmentation by capturing consumer behaviors such as shopping habits and social interactions (Parwekar & Gupta, 2019). This granular behavioral data support personalized targeting strategies (Vittala et al., 2024) and strengthen customer engagement, brand loyalty, and product positioning (Gawshinde et al., 2024; Taylor et al., 2020). Privacy-preserving techniques, including anonymization methods like *k*-anonymity, help maintain consumer trust while still allowing marketers to derive actionable insights (Gangrade, 2024). Neural network architectures further enhance marketing by analyzing complex datasets to refine segmentation and support data-driven decision-making.

In summary, these clusters show how technological innovations, ethical safeguards, and strategic opportunities transform STP from a static, survey-based model into a dynamic, AI-enabled, and privacy-conscious framework (Shastri & Pandit, 2021).

According to thematic structure (Figure 3), the analysis of the research corpus also highlights a critical convergence between marketing technologies (MT), security imperatives and privacy protection. Emerging technologies such as blockchain and artificial intelligence (AI) are fundamental pillars for building a secure and transparent marketing ecosystem. On the one hand, blockchain technology offers a decentralized and tamper-proof register that improves security and transparency, thus promoting trust between brands and consumers (Alkahtani et al., 2021; Boukis, 2020; Dionysis et al., 2022). Blockchain is increasingly used to secure supply chains, verify the origin of products, authenticate customer identities, and manage digital assets, strengthening the reliability of marketing ecosystems (Ali & Sofi, 2022; Chen et al., 2021; Zhang et al., 2022). In addition, smart contracts, which are self-executing agreements stored on the blockchain, make it possible to streamline processes, ensure transparency, and reduce the risks of fraud (Bodorik et al., 2023).

On the other hand, as marketing becomes more and more data-driven, AI plays a central role in protecting customer information and maintaining the integrity of marketing operations (Alhitmi et al., 2024; Cheng et al., 2023). AI-based systems are already being deployed to detect fraud, identify malicious activities, and strengthen security in various applications, such as online advertising, e-commerce, and customer relationship management (Li et al., 2021; Nagaraj et al., 2023). ML algorithms, in particular, excel at analyzing large datasets to recognize fraudulent patterns and predict security threats, allowing proactive risk mitigation (Pour et al., 2020; Sukhoparov & Lebedev, 2023). Future research should also prioritize the development of robust ML algorithms, like those explored by Hammedi et al. (2022), that can efficiently manage noisy sensor data, detect anomalies, and protect against cyber threats.

However, the successful integration of these technologies fundamentally depends on transparency, trust, and adaptability. Public concerns about the use of data, highlighted by Ford et al. (2019) and Piao and Cui (2021), require transparent and user-centered approaches to build trust. Ayaz et al. (2024) emphasize the need for AI systems to maintain transparency and interpretability to facilitate data-based decision-making in customer relationship management. In addition, adaptability and continuous learning are crucial for AI-based marketing strategies to remain effective, a principle whose broader applicability is demonstrated in malware detection (Budiarto et al., 2022; O'Mahony et al., 2021; Uysal et al., 2022). Mishandling of large amounts of customer data can lead to privacy violations (Cooper et al., 2023; Lopes et al., 2020). To mitigate these risks, marketing strategies must integrate privacy preservation techniques including data anonymization, differential privacy, and federated learning (Senavirathne & Torra, 2020; Yadav & Kumar, 2025), thus making it possible to take advantage of the advantages of AI and blockchain while protecting consumer information (Radanliev et al. 2024).

This conflict between personalization and confidentiality manifests acutely in specific applications like customer segmentation and positioning. AI-based segmentation makes it possible to offer more relevant experiences, whether in e-commerce, tourism, or smart building management (Naser et al., 2020; Penagos-Londoño et al., 2021; Peng & Xin, 2019). However, this practice raises crucial privacy issues. Solutions are emerging to manage this tension, notably integrating the notion of trust directly into algorithms, exemplified by the SPMF algorithm which segments users according to their preferences and their trust relationships (Peng & Xin, 2019). Another approach consists in segmenting individuals according to their perception of trust (Penagos-Londoño et al., 2021), or using privacy-friendly equipment as soon as data are collected, including thermal sensor networks that allow segmentation without visually identifying people (Naser et al., 2020). Likewise, the link between positioning and security is inherently complex. On the one hand, the collection of precise location data is confronted with fundamental confidentiality barriers, illustrated by the reluctance of companies to share GPS data deemed confidential (Greaves & Figliozzi, 2008). On the other hand, the security of positioning is actively threatened by attacks, a particularly critical threat in vehicle-to-vehicle communications (Nguyen et al., 2019) and WSN. To meet this challenge, strategic approaches based on game theory are proposed in order to balance the level of security and resource consumption (Esposito & Choi, 2017).

In conclusion, the interaction of AI, blockchain, and other advanced technologies shape the future of security in marketing. While these innovations offer unprecedented opportunities, their ethical deployment requires a commitment to transparency, privacy protection, and continuous adaptation (Manda et al., 2024; Sachdev, 2020; Thomaz et al., 2019). The constraints and risks linked to positioning, in particular, have direct implications for segmentation and targeting strategies. It is therefore imperative for marketing managers to integrate data governance and cyber-security considerations into their STP processes to strengthen consumer confidence and ensure regulatory compliance.

6. Conclusions, limitations, and recommendations

This article examines the intersection of MT, privacy, security, and marketing, with a particular emphasis on studies illustrating how these technologies are transforming marketing strategies while addressing security risks and safeguarding consumer data privacy. Privacy and security have become pivotal concerns in the domain of MT, drawing increasing interest from both academic and industry stakeholders. Despite their relevance across fields such as computer science, engineering, and marketing, the literature on these topics remains fragmented.

To address this gap, the present study offers a bibliometric analysis focused on privacy and security challenges within STP strategies. Analyzing 1,057 publications retrieved from the WoS database spanning 1996–2023, this research identifies notable gaps, particularly the need for further inquiry into ethical AI implementation, data transparency, and adaptive security frameworks.

A key limitation of this study lies in its exclusive reliance on the WoS database. Broader inclusion of repositories such as Scopus, IEEE Xplore, and SpringerLink could enrich the analysis and yield a more comprehensive understanding of the field.

The co-citation network analysis reveals three primary research clusters – IoT devices, privacy-preserving techniques, and neural network architectures – underscoring the interdisciplinary nature of MT-related marketing scholarship. These clusters demonstrate how technological innovation, ethical imperatives, and strategic design converge to shape the development of privacy-conscious marketing strategies.

The thematic map analysis, grounded in keyword frequency and co-occurrence patterns, reveals four principal clusters: (1) basic themes, primarily centered on security; (2) core themes, with privacy as a central focus; (3) niche themes, highlighting the role of sensors and related technologies in addressing privacy and security concerns; and (4) emerging themes, emphasizing the intersection of ML and privacy-focused marketing strategies. This structured classification offers a comprehensive view of how privacy and security issues are evolving within mobile marketing research.

The findings indicate that the effective integration of MT into marketing strategies depends on fostering transparency, building consumer trust, and maintaining adaptability. AI and blockchain technologies are expected to assume increasingly critical roles in securing marketing ecosystems; however, their ethical implementation necessitates robust privacy protections and the capacity for continuous adaptation.

Based on the studies that built the identified clusters, this article outlines research gaps and proposes a series of concrete and testable proposals that guide marketing managers and researchers. In today's data-intensive marketing landscape, it is increasingly important for managers and marketing researchers to integrate robust data governance and cybersecurity considerations into every stage of the STP process. This integration helps build consumer trust in location-based and personalized campaigns, while ensuring alignment with current privacy regulations. To achieve this, marketers should actively collaborate with IT and data governance teams. Such interdisciplinary cooperation enables the design of customer journeys that are both context-aware and compliant with privacy standards, while maintaining high levels of security. Aligning technological safeguards with marketing strategies contributes to a more resilient and trustworthy brand-consumer relationship.

Finally, future research should focus on bridging the identified gaps by developing innovative approaches to MT that enhance data security and consumer trust. As digital marketing continues to evolve, addressing these challenges will be essential to ensuring the sustainable and ethical use of mobile and AI-driven technologies in marketing.

Funding information

Authors state no funding involved.

Author contributions

All authors jointly contributed to all aspects of the research and manuscript preparation, including conceptualization, methodology, analysis, and writing. All authors reviewed and approved the final version of the manuscript.

Conflict of interest statement

Authors state no conflict of interest.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. doi: 10.1109/COMST.2015.2444095.

Alhitmi, H. K., Mardiah, A., Al-Sulaiti, K. I., & Abbas, J. (2024). Data security and privacy concerns of AI-driven marketing in the context of economics and business field: An exploration into possible solutions. *Cogent Business & Management*, *11*(1), 2393743. doi: 10.1080/23311975.2024.2393743.

Ali, J., & Sofi, S. A. (2022). Blockchain enabled architecture with selective consensus mechanisms for iot based saffron-agri value chain. *Scalable computing-practice and experience* (Vol. 23, Issues 4, pp. 457–472). Univ Vest Timișoara, West Univ Timișoara. doi: 10.12694/scpe.v23i4.2038.

Alkahtani, M., Khalid, Q. S., Jalees, M., Omair, M., Hussain, G., & Pruncu, C. I. (2021). E-agricultural supply chain management coupled with blockchain effect and cooperative strategies. *Sustainability*, *13*(2), 816. doi: 10.3390/su13020816.

AlRyalat, S. A., Malkawi, L., & Momani, S. (2019). Comparing bibliometric analysis using PubMed, scopus, and web of science databases. *Journal of Visualized Experiments*, *152*, e58494. doi: 10.3791/58494.

Aria, M., & Cuccurullo, C. (2017, November). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. doi: 10.1016/j.joi.2017.08.007.

Ayaz, T. B., Özara, M. F., Sezer, E., Çelik, A. E., & Akbulut, A. (2024, July). Enhancing targeting in CRM campaigns through explainable AI. In *International Conference on Intelligent and Fuzzy Systems* (pp. 203–214). Springer Nature Switzerland. doi: 10.1007/978-3-031-70018-7_23.

Bakar, M. S. A., & Bidin, R. (2014). Technology acceptance and purchase intention towards movie mobile advertising among youth in Malaysia. *Procedia-Social and Behavioral Sciences*, *130*, 558–567. doi: 10.1016/j.sbspro.2014.04.065.

Banerjee, S. (2019). Geosurveillance, location privacy, and personalization. *Journal of Public Policy & Marketing*, *38*(4), 484–499 doi: 10.1177/0743915619860137.

Benslama, T., & Jallouli, R. (2020, June). Clustering of social media data and marketing decisions. In *International Conference on Digital Economy* (pp. 53–65). Springer International Publishing. doi: 10.1007/978-3-030-64642-4_5.

Benslama, T., & Jallouli, R. (2022). Social media data analytics for marketing strategies: The path from data to value. *Journal of Telecommunications and the Digital Economy*, *10*(2), 96–110. doi: 10.18080/jtde.v10n2.523.

Benslama, T., & Jallouli, R. (2024). An empirical study of the impact of social media data analytics on marketing strategy: Which social media data analytics metrics to select?. *Journal of Telecommunications and the Digital Economy*, *12*(1), 575–594. doi: 10.18080/jtde.v12n1.830.

Beresford, A. R., & Stajano, F. (2004). Location privacy in pervasive computing. *IEEE Pervasive Computing*, *2*(1), 46–55. doi: 10.1109/MPRV.2003.1186725.

Bodorik, P., Liu, C., & Jutla, D. (2023). TABS: Transforming automatically BPMN models into blockchain smart contracts. *Blockchain: Research and Applications*, *4*(1), 100115. doi: 10.1016/j.bcra.2022.100115.

Boukis, A. (2020). Exploring the implications of blockchain technology for brand-consumer relationships: A future research agenda. *Journal of Product and Brand Management*, *29*(3), 307320. doi: 10.1108/JPBM-03-2018-1780.

Buck, C., & Burster, S. (2017). App information privacy concerns. *Twenty-third Americas Conference on Information Systems*.

Budiarto, R., Alqarni, A. A., Alzahrani, M. Y., Pasha, M. F., Firdhous, M. F. M., & Stiawan, D. (2022). User behavior traffic analysis using a simplified memory-prediction framework. *Computers, Materials and Continua*, *70*(2), 2679–2698. doi: 10.32604/cmc.2022.019847.

Callon, M., Courtial, J. P., & Laville, F. (1991). Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemistry. *Scientometrics*, *22*(1), 155–205. doi: 10.1007/BF02019280.

Capkun, S., & Hubaux, J.-P. (2006). Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 221–232. doi: 10.1109/JSAC.2005.861380.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys and Tutorials*, *21*(3), 2671–2701. doi: 10.1109/COMST.2019.2896380.

Chen, C.-L., Deng, Y.-Y., Weng, W., Zhou, M., & Sun, H. (2021). A blockchain-based intelligent anti-switch package in tracing logistics systems. *The Journal of Supercomputing*, *77*(7), 7791–7832. doi: 10.1007/s11227-020-03558-7.

Cheng, X., Liu, T., Shu, F., Ma, C., Li, J., & Wang, J. (2022). Providing location information at edge networks: A federated learning-based approach. *IEEE Network*, *36*(5), 114–120. doi: 10.1109/MNET.001.2200212.

Cheng, Y., Mei, S., Zhong, W., & Gao, X. (2023). Managing consumer privacy risk: The effects of privacy breach insurance. *Electronic Commerce Research*, *23*(2), 807–841. doi: 10.1007/s10660-021-09492-x.

Cheng, W. M., & Wang, S. M. (2021). Research on the general algorithm and benefit of real-time positioning advertising system-based on the use of 5G base station data. *Future Internet*, *13*(8), 187. doi: 10.3390/fi13080187.

Clark, J., Paiement, J. F., & Provost, F. (2023). Who's watching TV? *Information Systems Research*, *34*(4), 1622–1640. doi: 10.1287/isre.2023.1204.

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field. *Journal of Informetrics*, *5*(1), 146–166. doi: 10.1016/j.joi.2010.10.002.

Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2023). Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, *40*(2), 235–247. doi: 10.1108/JCM-04-2021-4577.

De Sousa, A., Moro, S., Pereira, R., & Prati, A. (2023). Cluster-based approaches toward developing a customer loyalty program in a private security company. *Applied Sciences (Basel)*, *14*(1), 78. doi: 10.3390/app14010078.

Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., & Fei-Fei, L. (2009). ImageNet: A large-scale hierarchical image database. *2009 IEEE Conference on Computer Vision and Pattern Recognition* (pp. 248–255). doi: 10.1109/CVPR.2009.5206848.

Dhar, S., & Bose, I. (2020). Securing IoT devices using zero trust and blockchain. *Journal of Organizational Computing and Electronic Commerce*, *31*(1), 18–34. doi: 10.1080/10919392.2020.1831870.

Dionysis, S., Chesney, T., & McAuley, D. (2022). Examining the influential factors of consumer purchase intentions for blockchain traceable coffee using the theory of planned behaviour. *British Food Journal*, *124*(12), 4304–4322. doi: 10.1108/BFJ-05-2021-0541.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296. doi: 10.1016/j.jbusres.2021.04.070.

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In S. Halevi & T. Rabin (Eds.), *Theory of cryptography* (Vol. 3876, pp. 265–284). Springer Berlin Heidelberg. doi: 10.1007/11681878_14.

Ebrahimi, F., Tushev, M., & Mahmoud, A. (2021). Mobile app privacy in software engineering research: A systematic mapping study. *Information and Software Technology*, *133*, 106466. doi: 10.1016/j.infsof.2020.106466.

Egghe, L. (2006, October). Theory and practice of the g-index. *Scientometrics*, *69*(1), 131–152. doi: 10.1007/s11192-006-0144-7.

Esposito, C., & Choi, C. (2017). Signaling game based strategy for secure positioning in wireless sensor networks. *Pervasive and Mobile Computing*, *40*, 611–627. doi: 10.1016/j.pmcj.2017.06.025.

Ford, E., Curlewis, K., Wongkoblap, A., & Curcin, V. (2019). Public opinions on using social media content to identify users with depression and target mental health care advertising: Mixed methods survey. *JMIR Mental Health*, *6*(11), e12942. doi: 10.2196/12942.

Gambetti, P., Roccazzella, F., & Vrins, F. (2022). Meta-learning approaches for recovery rate prediction. *Risks*, *10*(6), 124. doi: 10.3390/risks10060124.

Gangrade, P. (2024). Suggesting new techniques and methods for big data analysis: Privacy-preserving data analysis techniques. In *Big data analytics techniques for market intelligence* (pp. 265–291). IGI Global Scientific Publishing. doi: 10.4018/979-8-3693-0413-6.ch010.

Gao, S., & Zang, Z. (2016). An empirical examination of users' adoption of mobile advertising in China. *Information Development*, *32*(2), 203–215. doi: 10.1177/0266666914550113.

Gawshinde, S., Khurana, A., Kaur, H., & Kaur, S. (2024, December). Harnessing IoT data for real-time marketing insights and consumer engagement. In *International Conference on Leveraging Emerging Technologies and Analytics for Development* (pp. 355–371). Springer Nature Singapore. doi: 10.1007/978-981-96-2548-2_18.

Greaves, S. P., & Figliozzi, M. A. (2008). Collecting commercial vehicle tour data with passive global positioning system technology: Issues and potential applications. *Transportation Research Record*, *2049*(1), 158–166. doi: 10.3141/2049-19.

Gruteser, M., & Grunwald, D. (2003, May). Anonymous usage of location-based services through spatial and temporal cloaking. *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, (pp. 31–42). doi: 10.1145/1066116.1189037.

Hammedi, W., Brik, B., & Senouci, S. M. (2022). Toward optimal MEC-based collision avoidance system for cooperative inland vessels: A federated deep learning approach. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2525–2537. doi: 10.1109/TITS.2022.3154158.

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 770–778). doi: 10.1109/CVPR.2016.90.

Hentati, A., Jallouli, R. (2024, May). Diagnosing mobile banking applications to optimize user experience and engagement method, features and recommendations. In *International Conference on Digital Economy* (pp. 244–266). Springer Nature Switzerland. doi: 10.1007/978-3-031-76368-7_16.

Hirsch, J. E. (2005). An index to quantify an individual's scientific research output. *Proceedings of the National Academy of Sciences*, *102*(46), 16569–16572. doi: 10.1073/pnas.0507655102.

Hoh, B., Gruteser, M., Xiong, H., & Alrabady, A. (2010). Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking. *IEEE Transactions on Mobile Computing*, *9*(8), 1089–1107. doi: 10.1109/TMC.2010.62.

Hu, C., Song, M., & Guo, F. (2019). Intellectual structure of market orientation: A citation/co-citation analysis. *Marketing Intelligence & Planning*, *37*(6), 598–616. doi: 10.1108/MIP-08-2018-0325.

Huo, Z., Wang, T., Fan, Y., & He, P. (2023). Privacy-preserving global user profile construction through federated learning. *International Journal of Computational Science and Engineering*, *26*(2), 199–209. doi: 10.1504/IJCSE.2023.129739.

Kalnis, P., Ghinita, G., Mouratidis, K., & Papadias, D. (2007). Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering*, *19*(12), 1719–1733. doi: 10.1109/TKDE.2007.190662.

Kong, X. J., Gao, H. R., Shen, G. J., Duan, G. H., & Das, S. K. (2022). FEDVCP: A federated-learning-based cooperative positioning scheme for social Internet of vehicles. *IEEE Transactions on Computational Social Systems*, *9*(1), 1–10. doi: 10.1109/TCSS.2021.3062053.

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779–796. doi: 10.1016/j.future.2019.05.041.

Koubaa, H., Ben Said, F., & Jallouli, R. (2024, May). Bibliometric analysis and network mapping on mobile technologies in the area of marketing: Emerging topics and research recommendations. In *International Conference on Digital Economy* (pp. 339–365). Springer Nature Switzerland. doi: 10.1007/978-3-031-76365-6_20.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, *60*(6), 84–90. doi: 10.1145/3065386.

Kumar, R., Khan, A. A., Kumar, J., Zakria, Golilarz, N. A., Zhang, S., Ting, Y., Zheng, C., & Wang, W. (2021). Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Sensors Journal*, *21*(14), 16301–16314. doi: 10.1109/JSEN.2021.3076767.

Lakshmi, V. R. V., & Kumar, T. G. (2017). Mobile social networks: Architecture, privacy, security issues and solutions. *Journal of Communications*, *12*(9), 524–531. doi: 10.12720/jcm.12.9.524-531.

Li, C., Fu, Y., Yu, F. R., Luan, T. H., & Zhang, Y. (2020). Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. *IEEE Transactions on Intelligent Transportation Systems*, *22*(2), 898–912. doi: 10.1109/TITS.2019.2961400.

Li, Z., Hui, P., Zhang, P., Huang, J., Wang, B., Tian, L., Zhang, J., Gao, J., & Tang, X. (2021, April). What happens behind the scene? Towards fraud community detection in e-commerce from online to offline. In *Companion Proceedings of the Web Conference 2021* (pp. 105–113). doi: 10.1145/3442442.3451147.

Liu, H., Tian, Y., Peng, C., & Wu, Z. (2023). Privacy-utility equilibrium data generation based on Wasserstein generative adversarial networks. *Information Sciences*, *642*, 119069. doi: 10.1016/j.ins.2023.119069.

Lopes, H., Pires, I. M., San Blas, H. S., García-Ovejero, R., & Leithardt, V. (2020). Priada: Management and adaptation of information based on data privacy in public environments. *Computers*, *9*(4), 77. doi: 10.3390/computers9040077.

Majzoubi, M., & Zhao, E. Y. (2023). Going beyond optimal distinctiveness: Strategic positioning for gaining an audience composition premium. *Strategic Management Journal*, *44*(4), 907–931. doi: 10.1002/smj.3460.

Manda, V. K., Sagi, S., & Yadav, A. (2024). Blockchain in advertising and marketing: Revolutionizing the industry through transparency and trust. In *New trends in marketing and consumer science* (pp. 89–112). IGI Global. doi: 10.4018/979-8-3693-2754-8.ch005.

Mao, B., Liu, J., Wu, Y., & Kato, N. (2023). Security and privacy on 6G network edge: A survey. *IEEE Communications Surveys & Tutorials*, *25*(2), 1095–1127. doi: 10.1109/COMST.2023.3244674.

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22. doi: 10.1109/MPRV.2018.03367731.

Meyer, N., Ben Said, F., Alkathiri, N. A., & Soliman, M. (2023). A scientometric analysis of entrepreneurial and the digital economy scholarship: State of the art and an agenda for future research. *Journal of Innovation and Entrepreneurship*, *12*(1), 70. doi: 10.1186/s13731-023-00340-w.

Michael, K., & Clarke, R. (2013). Location and tracking of mobile devices: Uberveillance stalks the streets. *Computer Law & Security Review*, *29*(3), 216–228. doi: 10.1016/j.clsr.2013.03.004.

Milne, G., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment- and technology-level analysis. *Journal of Public Policy & Marketing*, *29*(1), 138–148. doi: 10.1509/jppm.29.1.138.

Nagaraj, P., Muneeswaran, V., Dharanidharan, A., Aakash, M., Balananthanan, K., & Rajkumar, C. (2023, January). E-commerce customer churn prediction scheme based on customer behaviour using machine learning. In *2023 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–6). IEEE. doi: 10.1109/ICCCI56745.2023.10128498.

Nanni, M., Trasarti, R., Monreale, A., Grossi, V., & Pedreschi, D. (2016). Driving profiles computation and monitoring for car insurance CRM. *ACM Transactions on Intelligent Systems and Technology*, *8*(1), 26. doi: 10.1145/2912148.

Narang, U., & Shankar, V. (2019). Mobile marketing 2.0: State of the art and research agenda. *Marketing in a Digital World* (pp. 97–119). Emerald Publishing Limited. doi: 10.1108/S1548-643520190000016008.

Naser, A., Lotfi, A., & Zhong, J. (2020). Adaptive thermal sensor array placement for human segmentation and occupancy estimation. *IEEE Sensors Journal*, *21*(2), 1993–2002. doi: 10.1109/JSEN.2020.3020401.

Nguyen, V.-L., Lin, P.-C., & Hwang, R.-H. (2019). Multi-array relative positioning for verifying the truthfulness of V2X messages. *IEEE Communications Letters*, *23*(10), 1704–1707. doi: 10.1109/LCOMM.2019.292797.

Orouji, N., & Mosavi, M. R. (2020). Novel secure positioning method in ultra-wide band framework based on overshadowing attack probabilistic model. *IET Communications*, *14*(1), 1–10. doi: 10.1049/iet-com.2019.1138.

Ozturk, O. (2021). Bibliometric review of resource dependence theory literature: An overview. *Management Review Quarterly*, *71*(3), 525–552. doi: 10.1007/s11301-020-00192-8.

O'Mahony, G. D., McCarthy, K. G., Harris, P. J., & Murphy, C. C. (2021). Developing novel low complexity models using received in-phase and quadrature-phase samples for interference detection and classification in wireless sensor network and GPS edge devices. *Ad Hoc Networks*, *120*, 102562. doi: 10.1016/j.adhoc.2021.102562.

Parwekar, P., & Gupta, G. (2019). Cloud data for marketing in tourism sector. In *Smart Trends in Computing and Communications: Proceedings of SmartCom 2019* (pp. 143–153). Springer Singapore. doi: 10.1007/978-981-15-0077-0_16.

Penagos-Londoño, G. I., Rodriguez–Sanchez, C., Ruiz-Moreno, F., & Torres, E. (2021). A machine learning approach to segmentation of tourists based on perceived destination sustainability and trustworthiness. *Journal of Destination Marketing & Management*, *19*, 100532. doi: 10.1016/j.jdmm.2020.100532.

Peng, T., Liu, Q., & Wang, G. (2014). Enhanced location privacy preserving scheme in location-based services. *IEEE Systems Journal*, *11*(1), 219–230. doi: 10.1109/JSYST.2014.2354235.

Peng, W., & Xin, B. G. (2019). A social trust and preference segmentation-based matrix factorization recommendation algorithm. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 272. doi: 10.1186/s13638-019-1600-4.

Piao, Y. J., & Cui, D. Y. (2021). Privacy analysis and comparison of pandemic contact tracing apps. *KSII Transactions on Internet and Information Systems*, *15*(11), 4145–4162. doi: 10.3837/tiis.2021.11.015.

Poddar, S. D., Murali, M., Rajasekaran, P., & Prabakaran, N. (2024, March). A comprehensive study on security threats in autonomous vehicles: Safeguarding the future. In *2024 1st International Conference on Cognitive, Green and Ubiquitous Computing (IC-CGU)* (pp. 1–6). IEEE. doi: 10.1109/IC-CGU58078.2024.10530760.

Pour, M. S., Mangino, A., Friday, K., Rathbun, M., Bou-Harb, E., Iqbal, F., Samtani, S., Crichigno, J., & Ghani, N. (2020). On data-driven curation, learning, and analysis for inferring evolving Internet-of-Things (IoT) botnets in the wild. *Computers & Security*, *91* 101707. doi: 10.1016/j.cose.2019.101707.

Pranckutė, R. (2021). Web of science (WoS) and scopus: The titans of bibliographic information in today's academic world. *Publications*, *9*(1), 12. doi: 10.3390/publications9010012.

Purwanto, E., Deviny, J., & Mutahar, A. M. (2020). The mediating role of trust in the relationship between corporate image, security, word of mouth and loyalty in M-banking using among the millennial generation in Indonesia. *Management & Marketing*, *15*(2), 255–274. doi: 10.2478/mmcks-2020-0016.

Radanliev, P., Santos, O., Brandon-Jones, A., & Joinson, A. (2024). Ethics and responsible AI deployment. *Frontiers in Artificial Intelligence*, *7*, 1377011. doi: 10.3389/frai.2024.1377011.

Rafieian, O., & Yoganarasimhan, H. (2021). Targeting and privacy in mobile advertising. *Marketing Science*, *40*(2),193–218. doi: 10.1287/mksc.2020.1235.

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, *11*(8), 2661–2674. doi: 10.1016/j.adhoc.2013.04.014.

Sachdev, R. (2020, April). Towards security and privacy for edge AI in IoT/IoE based digital marketing environments. In *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 341–346). IEEE. doi: 10.1109/FMEC49853.2020.9144755.

Sakas, D. P., & Giannakopoulos, N. T. (2021). Big data contribution in desktop and mobile devices comparison, regarding airlines' digital brand name effect. *Big Data and Cognitive Computing*, *5*(4), 48. doi: 10.3390/bdcc5040048.

Senavirathne, N., & Torra, V. (2020, December). On the role of data anonymization in machine learning privacy. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 664–675). IEEE. doi: 10.1109/TrustCom50675.2020.00093.

Serrano-Malebran, J., Vidal-Silva, C., & Veas-González, I. (2023). Social media marketing as a segmentation tool. *Sustainability*, *15*(2), 1151. doi: 10.3390/su15021151.

Shastri, M. D., & Pandit, A. A. (2021). Remodeling: Improved privacy preserving data mining (PPDM). *International Journal of Information Technology*, *13*(1), 131–137. doi: 10.1007/s41870-020-00531-8.

Shi, Y., Siddik, A., Masuku, M., Zheng, G. W., Hamayun, M., & Ibrahim, A. M. (2022). The antecedents of willingness to adopt and pay for the IoT in the agricultural industry: An application of the UTAUT 2 theory. *Sustainability*, *14*(11), 6640. doi: 10.3390/su14116640.

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*. doi: 10.48550/arXiv.1409.1556.

Simpson, B. (2014). Tracking children, constructing fear: GPS and the manufacture of family safety. *Information & Communications Technology Law*, *23*(2), 273–285 doi: 10.1080/13600834.2014.970377.

Sinha, M., Majra, H., Hutchins, J., & Saxena, R. (2019). Mobile payments in India: The privacy factor. *International Journal of Bank Marketing*, *37*(1), 192–209. doi: 10.1108/IJBM-05-2017-0099.

Song, Y., Fu, Y., Yu, F. R., & Zhou, L. (2020). Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach. *IEEE Internet of Things Journal*, *7*(4), 3485–3498. doi: 10.1109/JIOT.2020.2972337.

Srivastava, P. R., Sharma, D., Kaur, I., & Wamba, S. F. (2021). Intellectual structure and publication pattern in journal of global information management: A bibliometric analysis during 2002–2020. *Journal of Global Information Management (JGIM)*, *29*(4), 1–31. doi: 10.4018/JGIM.20210701.oa1.

Stachl, C., Au, Q., Schoedel, R., Gosling, S., Harari, G., Buschek, D., Völkel, S. T., Schuwerk, T., Oldemeier, M., Ullmann, T., & Hussmann, H. (2020). Predicting personality from patterns of behavior collected with smartphones. *Proceedings of the National Academy of Sciences*, *117*(30), 17680–17687. doi: 10.1073/pnas.1920484117.

Sukhoparov, M. E., & Lebedev, I. S. (2023) Improving the quality of the identification of the information security state based on sample segmentation. *Automatic Control and Computer Sciences*, *57*(8), 1071–1075. doi: 10.3103/S0146411623080321.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5), 557–570. doi: 10.1142/S0218488502001648.

Taylor, M., Reilly, D., & Wren, C. (2020). Internet of things support for marketing activities. *Journal of Strategic Marketing*, *28*(2), 149–160. doi: 10.1080/0965254X.2018.1493523.

Teodorescu, C. A., Ciurea, C. E., Saftiuc, B. P., & Staicu, D. (2025), The evolution of mobile cybersecurity regulations in the European Union. *Management & Marketing*, *20*(1), 52–63. 10.2478/mmcks-2025-0004.

Thakur, R., & Srivastava, M. (2013). Customer usage intention of mobile commerce in India: An empirical study. *Journal of Indian Business Research*, *5*(1), 52–72. doi: 10.1108/17554191311303385.

Thangavel, P., & Chandra, B. (2023). Two decades of M-commerce consumer research: A bibliometric analysis using R biblioshiny. *Sustainability*, *15*(15), 11835 doi: 10.3390/su151511835.

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2019, November 11). Learning from the Dark Web: Leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, *48*(1), 43–63. doi: 10.1007/s11747-019-00704-3.

Ullah, I., Boreli, R., & Kanhere, S. S. (2023). Privacy in targeted advertising on mobile devices: A survey. *International Journal of Information Security*, *22*(3), 647–678 doi: 10.1007/s10207-022-00655-x.

Uysal, D. T., Yoo, P. D., & Taha, K. (2022). Data-driven malware detection for 6G networks: A survey from the perspective of continuous learning and explainability via visualization. *IEEE Open Journal of Vehicular Technology*, *4*, 61–71. doi: 10.1109/OJVT.2022.3219898.

Van Angeren, J., Vroom, G., McCann, B. T., Podynitsyna, K., & Langerak, F. (2022). Optimal distinctiveness across revenue models: Performance effects of differentiation of paid and free products in a mobile app market. *Strategic Management Journal*, *43*(10), 2066–2100. doi: 10.1002/smj.3394.

Varnali, K., & Toker, A. (2010). Mobile marketing research: The-state-of-the-art. *International Journal of Information Management*, *30*(2), 144–151. doi: 10.1016/j.ijinfomgt.2009.08.009.

Vittala, K. P., Kumar, K., Seranmadevi, R., & Tyagi, A. K. (2024). Artificial intelligence-Internet of Things integration for smart marketing: Challenges and opportunities. *Advancing software engineering through AI, federated learning, and large language models* (pp. 295–307). IGI Global. doi: 10.4018/979-8-3693-3502-4.ch019.

Wang, Y., Liu, Q., Mihankhah, E., Lv, C., & Wang, D. (2021). Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation. *IEEE Transactions on Intelligent Transportation*

Systems, *23*(7), 8247–8259. doi: 10.1109/TITS.2021.3077015.

Wu, H. T. (2022). The Internet-of-Vehicle traffic condition system developed by artificial intelligence of things. *Journal of Supercomputing*, *78*(2), 2665–2680. doi: 10.1007/s11227-021-03969-0.

Yadav, A., & Kumar, A. (2025). Mobile data anonymization in cyber security: Techniques, applications, and future directions. In *Artificial intelligence for cyber security and industry 4.0* (pp. 343–370). CRC Press. doi: 10.1201/9781032657264-15.

Yang, Y., & Kels, C. (2016). Does the shoe fit? Ethical, legal, and policy considerations of global positioning system shoes for individuals with Alzheimer's disease. *Journal of the American Geriatrics Society*, *64*(8), 1708–1715. doi: 10.1111/jgs.14265.

Zakroum, M., Francois, J., Chrisment, I., & Ghogho, M. (2022). Monitoring network telescopes and inferring anomalous traffic through the prediction of probing rates. *IEEE Transactions on Network and Service Management*, *19*(4), 5170–5182. doi: 10.1109/TNSM.2022.3183497.

Zhang, G., Chen, X., Zhang, L., Feng, B., Guo, X., Ling, J., & Zhang, Y. (2022). STAIBT: Blockchain and CP-ABE empowered secure and trusted agricultural IoT blockchain terminal. *IJIMAI*, *7*(5), 66–75. doi: 10.9781/ijimai.2022.07.004.

Zhang, J. Z., Srivastava, P. R., Sharma, D., & Eachempati, P. (2021). Big data analytics and machine learning: A retrospective overview and bibliometric analysis. *Expert Systems with Applications*, *184*, 115561. doi: 10.1016/j.eswa.2021.115561.

Zhu, J., & Liu, W. (2020). A tale of two databases: The use of Web of Science and Scopus in academic papers. *Scientometrics*, *123*(1), 321–335. doi: 10.1007/s11192-020-03387-8.

Zhu, Y., Liu, Y., Yu, J., & Yuan, X. (2021). Semi-supervised federated learning for travel mode identification from GPS trajectories. *IEEE Transactions on Intelligent Transportation Systems*, *23*(3), 2380–2391. doi: 10.1109/TITS.2021.3092015.

Appendices

Search query	Web of science type	Date	Selected documents
1# (TI = ("Marketing strategies" OR "Segmentation" OR "Positioning" OR "Targeting") OR AB = ("Marketing strategies" OR "Segmentation" OR "Positioning" OR "Targeting") OR AK = ("Marketing strategies" OR "Segmentation" OR "Positioning" OR "Targeting"))	Core collection	30-Jun-24	995,170
2# (TI = ("Machine Learning" OR "AI" OR "IoT" OR "Blockchain" OR "Recommender Systems" OR "Mobile Store" OR "Mobile applications" OR "Artificial neural network" OR "Genetic algorithms" OR "GPS" OR "Radio frequency identification" OR "RFID" OR "Sensor networks" OR "Tracking technologies" OR "cookies" OR "clear gifs") OR AB = ("Machine Learning" OR "AI" OR "IoT" OR "Blockchain" OR "Recommender Systems" OR "Mobile Store" OR "Mobile applications" OR "Artificial neural network" OR "Genetic algorithms" OR "GPS" OR "Radio frequency identification" OR "RFID" OR "Sensor networks" OR "Tracking technologies" OR "cookies" OR "clear gifs") OR AK = ("Machine Learning" OR "AI" OR "IoT" OR "Blockchain" OR "Recommender Systems" OR "Mobile Store" OR "Mobile applications" OR "Artificial neural network" OR "Genetic algorithms" OR "GPS" OR "Radio frequency identification" OR "RFID" OR "Sensor networks" OR "Tracking technologies" OR "cookies" OR "clear gifs"))	Core collection	30-Jun-24	933,830
3# (TI = ("Privacy" OR "Security" OR "Confidentiality" OR "Trust") OR AB = ("Privacy" OR "Security" OR "Confidentiality" OR "Trust") OR AK = ("Privacy" OR "Security" OR "Confidentiality" OR "Trust"))	Core collection	30-Jun-24	786,969
#1 AND #2 AND #3 and Article (Document Types) and English (Languages)	Core collection	30-Jun-24	1,185

Table A1. Document search process.

Source: Authors' own research.

Description	Results
Main information about data	
Time span	1996–2023
Sources (journals, books, etc.)	502
Documents	1057
Annual growth rate %	21.79
Document average age	4.61
Average citations per doc	18.22
References	42,078
Document contents	
Keywords plus (ID)	1,170
Author's keywords (DE)	3,798
Authors	
Authors	3,957
Authors of single-authored docs	56
Authors' collaboration	
Single-authored docs	56
Co-authors per doc	4.17
International co-authorships %	33.77

Table A2. Main indicators.

Source: Authors' own research.