Journal of Computer Science and Electrical Engineering
ISSN: 2663-1938
DOI: 10.61784/jcsee3018

COMPUTATIONAL BIG MODEL-BASED STUDY OF PRIVACY PROTECTION MECHANISMS AND PROBLEMATIC USAGE BEHAVIOUR IN DIGITAL MEDIA

Jin Lu[1], Ji Li[2*]
[1]*Guangdong Key Laboratory of Big Data Intelligence for Vocational Education, Shenzhen Polytechnic University, Shenzhen 518000, Guangdong, China.*
[2]*Research Management Office, Shenzhen Polytechnic University, Shenzhen 518000, Guangdong, China.*
Corresponding Author: Ji Li, Email: liji@szpu.edu.cn

Abstract: With the rapid development of information technology, digital media has become an important part of people's daily lives. From social media to online shopping, from cloud computing to artificial intelligence, digital media not only greatly enriches people's lifestyles, but also brings unprecedented data privacy protection challenges. In particular, the wide application of computational big models (e.g., deep learning models, natural language processing models, etc.) has further exacerbated the complexity of data privacy protection. This paper aims to explore the privacy protection mechanism of digital media based on computational big models and analyse the resulting problematic use behaviour, with a view to providing references for research and practice in related fields, delving into the development of the convergence of computational big models and digital media, analyzing the manifestation of problematic use behaviors and privacy issues in digital media, exploring the challenges and countermeasures to prevent the privacy issues, and presenting the challenges and countermeasures to prevent privacy issues in digital media privacy protection mechanism under the computational big model. Successful privacy protection experiences and lessons of problematic use behaviors leading to privacy issues are summarized through case studies. Finally, the research results are summarized and future trends and research directions are outlined.
Keywords: Big model; Privacy protection mechanisms; Usage behaviour; Digital media

1 INTRODUCTION

In the social media environment, leakage sources such as the user himself, other Internet users, platforms and third parties may cause the leakage of user privacy information. The characteristics of digital media's multi-subject participation (users, friends, and platforms) make user privacy protection strategies more complex. Traditional online privacy protection is mainly achieved through corporate privacy practices, industry self-regulation and government regulation, however, the effectiveness of such corporate privacy protection strategies is widely questioned in the era of big data. Based on the shortcomings of existing privacy protection strategies, the EU proposes an approach that integrates engineering and strategic management to achieve selective and continuous minimization of information system privacy risks through technical and regulatory controls, a strategy to minimize privacy risks through technology and controls from a system design perspective[1]. With the popularity of mobile devices, people are increasingly using various mobile applications in their daily lives, and the competition among mobile application developers is becoming more and more intense. For developers, the collection and use of user data has huge business potential and is the basis for realizing personalized services, so developers will ask users for authorization to collect some information during the process of opening or using the app. However, with the rapid changes in IT, which makes the data diffusion method hard to be predicted, users are not sure of the consequences of authorization and are worried about the misuse of their private information[2-3], and due to the frequent leakage of online users' information and privacy in recent years, users have become more and more cautious about authorizing information collection behaviors[4]. Therefore, it has been explored how to design and optimize the mobile APP authorization interface, and how to collect and use privacy information, so as to provide better services for users, which is crucial for both APP developers and users[5]. Data leakage will not only cause economic loss to enterprises, but also damage consumer satisfaction and purchase intention[6]. Therefore, the problem of remediation after data leakage has become an important challenge for the Internet industry. However, service remediation of privacy data leakage is different from traditional service remediation in that it is characterized by a large number of victims and an immeasurable loss[7]. As a result, companies are increasingly interested in how best to conduct data breach remediation.

With the emergence and popularity of smartphones, mobile social networks have become part of an individual's daily life, providing new ways of communicating, socializing and maintaining friendships, thus improving people's life experience. However, more and more people have started to show some tendencies of problematic use in uncontrollable ways in untimely scenarios. Problematic use refers to unplanned and impulsive use of digital media, which usually has a negative impact on the user[8]. Research has shown that problematic use of digital media is detrimental to people's real-life relationships[9], job performance[10], academic achievement[11], and subjective well-being[12], among others. Much of the literature has examined the triggers of problematic behaviors, focusing on individual psychological characteristics, but neglecting the role of technological media. Studies have shown that media characteristics play an

important role in influencing user behaviour[13]. Therefore, there is a need to investigate the role of media technologies so that users and practitioners can better understand problematic use of digital media.

Privacy-preserving mechanisms are essential in the digital media landscape to protect user data and prevent problematic usage behaviors. With the increasing use of mobile devices, monitoring users and building detailed profiles for behavioral advertising has become common practice[14]. Digital trace data collection allows for the analysis of content usage on social media platforms, shedding light on textual and audio-visual content[15]. The use of the internet and social media has changed consumer behavior, leading to eWOM overload that can be mitigated by new tools and mechanisms[16]. In the healthcare sector, digital transformation has led to the development of privacy-preserving smart healthcare frameworks based on blockchain technology[17]. The National Strategy to Advance Privacy-Preserving Data Sharing emphasizes the importance of federally funded research in networking and information technology to protect user data[18]. Privacy in targeted advertising on mobile devices is a growing concern, with research focusing on usage behavioral patterns and interest-based ads targeting[19]. In the digital sphere, privacy-preserving mechanisms are crucial for protecting private attributes and data flows related to media usage and marketplace behavior[20]. Big data privacy solutions, such as differential privacy and homomorphic encryption, have been developed to protect user data in content and social media analysis[21]. As digital platforms continue to impact news and journalistic content, research is needed to address privacy concerns and protect user data[22]. Overall, the intersection of privacy-preserving mechanisms and problematic usage behaviors in digital media highlights the importance of protecting user data and ensuring ethical practices in data collection and analysis. Solutions such as blockchain technology, differential privacy, and federated learning play a crucial role in safeguarding user privacy in the digital age[23].

This paper provides an in-depth study of the development of the convergence of computational big models and digital media. Chapter 2 analyses the behavioral manifestations of problematic use of digital media and privacy issues. Chapter 3 explores the challenges and countermeasures to prevent privacy issues and introduces the privacy protection mechanism of digital media under the computational big model. Chapter 4 summaries successful privacy protection experiences and lessons learned from problematic use behaviors leading to privacy issues through case studies. Finally, the research results are summarized and future trends and research directions are outlined.

2 THEORY AND PROGRAMME

The study of privacy-preserving mechanisms and problematic use behaviors of digital media based on computational macro-models is a complex topic covering multiple aspects, which involves a number of domains such as technology, ethics, law and social impact. While digital media satisfy people's needs, they also cause serious privacy leakage, and the process is defensible with complex features such as multiple sources, interaction, blocking, network externalizes and concealment. In order to gain access to digital media, gain the trust of online users or share life experiences, etc., people need to provide their personal information such as name, ID number, mobile phone number, geographic location, etc. online, and share life experiences and family photos, etc., and platforms and third parties may also obtain private information such as the user's interpersonal network, identity and preferences through association detection, data mining and other technologies. This study will examine the potential vulnerabilities and threats posed by the increasing volume and complexity of data in the context of big data analysis. Furthermore, the research will explore the impact of these vulnerabilities on the confidentiality, integrity, and availability of data, as well as the potential consequences for organizations and individuals. Moreover, the study will investigate the efficacy of current data security measures in mitigating these risks and propose recommendations for enhancing data protection strategies in the age of big data analysis. Additionally, the study will assess the role of data encryption, access controls, and authentication mechanisms in safeguarding data integrity and preventing unauthorized access in the context of big data analysis. Moreover, this research will also analyze the role of data governance frameworks and regulatory compliance in ensuring data security in the age of big data analysis. This study aims to provide a comprehensive analysis of the multifaceted challenges and implications of data security in the era of big data analysis, with a particular focus on the role of encryption, access controls, authentication mechanisms, data governance frameworks, and regulatory compliance in safeguarding data integrity and preventing unauthorized access. Furthermore, the research will delve into the intricate interplay between data security measures and organizational practices, aiming to offer a holistic understanding of the complexities involved in ensuring robust data protection in the era of big data analysis. This comprehensive analysis will shed light on the intricate interplay between data security measures and organizational practices, providing a holistic understanding of the complexities involved in ensuring robust data protection in the era of big data analysis. Next, several basic theories covered in this paper will be analyzed.

2.1 Computational Big Models in Digital Media

The application of computational big models in digital media mainly includes three aspects of content recommendation, automatic generation, speech recognition and image processing, which are shown in Table 1.

Table 1 Application and Classification of Computational Big Models in Digital Media

Element	Connotation Description
Content	One of the major applications of computational big models in digital media is content

Recommendations[24]	recommendation. Through in-depth analysis of user behaviour, content features and other data, the big model is able to recommend personalized content for users, such as news, videos, music and so on. This process requires the model to process a large amount of user data, including but not limited to browsing history, clicking behaviour, purchase records, etc.
Automatic Generation[25]	Computational Big Model also has the ability to automatically generate content such as press releases, articles, video scripts, etc. This not only reduces the cost of manual creation, but also increases the efficiency and diversity of content production. However, this automated generation process also involves processing and analysing large amounts of data such as text and images.
Speech Recognition and Image Processing[26]	In the field of speech recognition and image processing, computational big models play an equally important role. Through deep learning of speech signals and image data, the models are able to achieve high-precision speech-to-text, image classification, target detection and other functions. The realization of these functions relies on the processing of sensitive information such as the user's voice and facial features.

2.2 Digital Media Privacy Protection Mechanisms

The digital media privacy protection mechanism mainly includes three parts: the innovative application of encryption technology, the construction of intelligent defence system, and the formulation and implementation of privacy protection policy, as shown in Table 2.

Table 2 Categorical Description of Innovative Applications of Cryptography

Element	Connotation Description
Innovative applications of encryption[27]	In digital media, data encryption is an important means of protecting privacy. Traditional encryption methods, although effective, appear to be incompetent in the face of computationally large models. Therefore, it is necessary to develop more efficient and intelligent encryption models by combining deep learning techniques. For example, using deep learning algorithms to train efficient encryption models can improve the efficiency of data transmission and storage while ensuring data security. In addition, the introduction of techniques such as differential privacy can provide rich data resources for the training of computationally large models while protecting user privacy.
Construction of Intelligent Defence System[28]	Intelligent defence systems based on computational macro-models can monitor network traffic in real time, automatically identify and intercept malicious traffic, and effectively prevent network attacks. These systems are able to cope with increasingly complex and covert attack methods by continuously learning and optimizing their own defence strategies. In addition, a phishing detection solution built using encryption technology can analyse the content and structure of emails to identify potential phishing attacks and activate an early warning mechanism in the first instance.
Privacy Policy Development and Enforcement[29]	A sound privacy protection policy is the basis for safeguarding user privacy. In the age of digital media, the purpose of data collection and use must be clear and legitimate, and data subjects must grant explicit consent to the collection and use of their data. At the same time, data collectors must adopt appropriate security measures to protect personal data and prevent data leakage and misuse. Governments and relevant organizations should strengthen the regulation of data collection and use to ensure that data collectors comply with relevant regulations and policies.

2.3 Problematic Use Behaviour and its Coping Strategies

The problematic use behaviors can be classified into three categories: data misuse and leakage, lack of user privacy awareness, and privacy leakage under technological unconsciousness. These are outlined in Table 3, together with recommended coping strategies.

Table 3 Description of Problematic Use Behaviors and Their Coping Strategies

Element	Connotation Description	Response Strategies
Data Misuse and Compromise[30]	Data misuse and leakage are common privacy protection issues in digital media. Some unscrupulous elements or internal employees may take advantage of system loopholes or mismanagement to illegally obtain, use or leak user data. Such behaviour not only violates users' privacy, but may also cause property damage and mental harm to users.	● Enhance system security: Regularly check and fix system vulnerabilities to ensure system security and stability. ● Improve internal management: Strengthen security education and training for employees, and formulate strict regulations on data access and use to prevent internal leakage. ● Establish an emergency response mechanism: In the event of a data leakage

		incident, activate the emergency response mechanism in a timely manner to quickly identify the cause and take measures to reduce losses. ● Raise users' privacy awareness: Raise users' awareness of privacy protection through publicity and education, case sharing, etc., so that users understand the importance of personal privacy and how to protect it. ● Simplify privacy policies: Simplify complex privacy policies into easy-to-understand language to ensure that users can fully understand and agree to the content of the privacy policy. ● Introduce third-party certification mechanism: Improve user trust in digital media platforms by introducing a third-party certification organization to assess and certify the privacy protection capabilities of the platforms. ● Enhance technology transparency: Increase transparency in the use of technology so that users understand the process and possible risks of data collection, processing and use. ● Limit the scope of data collection: Clarify the purpose and scope of data collection and avoid collecting unnecessary data to minimize the risk of privacy breaches. ● Provide user control: Give users control over their data and allow them to view, modify or delete their data at any time.
Lack of user privacy awareness[31]	While enjoying the convenience of digital media, users often neglect the protection of their personal privacy. Some users casually disclose personal information due to a lack of awareness of privacy protection, or authorize third parties to access personal data without understanding privacy policies.	
Privacy breaches in the technological unconscious[32]	With the popularity of smart devices and the development of AI technology, a large amount of data is automatically exchanged between smart devices without the user's knowledge. This technological unconscious privacy leakage poses a great risk to users.	

2.4 Problematic

In order to solve the first problem raised in this paper, combined with the principal-agent theory, the permission request features (permission explanation, third-party authentication and permission relevance) are explored to influence user authorization behaviour by reducing the user's perceived uncertainty, and a research model, as in Figure 1, is established and examined through scenario-based experimental methods. In this case, permission explanation refers to explaining the purpose of information collection and how it is used to the user when asking for authorization. Permission relevance refers to the degree of relevance of the requested permission to the core functionality. Third-party authentication refers to authentication by an authority independent of the developer.

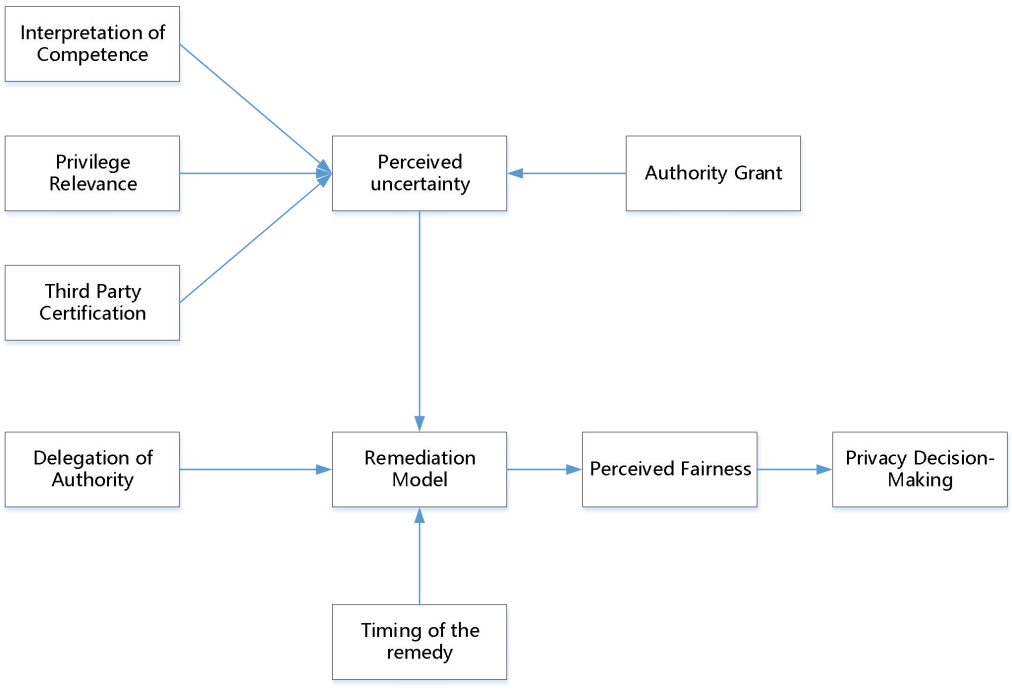

Figure 1 Model of the Effect of Authorization Interface Request Characteristics on Group Privacy Intentions

3 THE CONVERGENCE OF COMPUTATIONAL BIG MODELS AND DIGITAL MEDIA

In today's digital era, the rise of computational big models has brought profound changes to digital media. With its powerful data analysis and processing capabilities, Computational Big Model is able to quickly and accurately process large amounts of data such as text, images, audio and video, providing digital media with more accurate content recommendations, personalized services, and automatic generation of news, articles and videos. The emergence of computational big models not only improves the production efficiency and quality of digital media, but also provides users with a richer and more personalized media experience.

3.1 Application Areas of Computational Big Model in Digital Media

The application areas of computational big models in digital media include four sections such as content recommendation and personification, automatic generation of news, articles and videos, speech recognition and image processing, and sentiment analysis, as shown below.

3.1.1 Content recommendation and personalized services

Computing big models can provide personalized content recommendation and services for users by analyzing data such as users' historical behaviour, interests and social relationships. For example, a news client can recommend news articles of interest to users based on their reading history and interest preferences; a video platform can recommend personalized video content to users based on their viewing history and preferences.

3.1.2 Automatic generation of news, articles and videos.

Computational big models can automatically generate content such as news, articles and videos by learning from large amounts of text, image and video data. For example, some news organizations have started to use computational big models to automatically generate news stories, improving the efficiency and quality of news production.

3.1.3 Speech recognition and image processing

Computational Big Models can achieve functions such as speech recognition and image processing by learning a large amount of speech and image data. For example, voice assistants can provide users with voice interaction services through voice recognition technology; image recognition software can recognition information such as objects and people in images through image processing technology.

3.1.4 Sentiment analysis

Computing big models can achieve functions such as sentiment analysis by analyzing sentiment information in data such as text, voice and images. For example, social media platforms can use sentiment analysis technology to understand users' emotional inclination towards an event or topic, and provide decision-making references for enterprises and governments.

3.2 The Opportunities and Challenges of Computing Big Models for Digital Media

Through deep learning technology, the computational model can quickly generate high-quality content, such as news reports, articles, video scripts, etc., which greatly improves the production efficiency of media content. In terms of creative design, large models can generate illustrations, posters, advertisements and other visual elements, providing a rich source of material for the media industry.

3.2.1 Enhancing efficiency and innovation

The emergence of computational big models has brought unprecedented opportunities for digital media. Computational big models can process large amounts of data quickly and accurately, improving the production efficiency and quality of digital media. At the same time, computational big models can also provide digital media with more innovative services and functions, such as personalized recommendations and automatic content generation, to meet the changing needs of users.

3.2.2 Data security and privacy protection challenges

With the application of computational big models, digital media are facing increasingly severe data security and privacy protection challenges. Computational big models require a large amount of data for training and optimization, which may contain users' personal information and privacy. If these data are leaked or misused, it will have a serious impact on users' rights and interests and the stability of the society.

4 THE ANALYSIS OF THE BEHAVIOR AND PRIVACY OF THE DIGITAL MEDIA

Large models need to deal with a large amount of user data in the process of training and using, so how to protect user privacy and prevent data leakage has become an important issue.

4.1 The Definition of Digital Media Problematic Usage Behavior Based on Computational Big Model

4.1.1 Over-reliance on big models to generate content

Some digital media practitioners and users over-rely on computing big models to generate content, and lack of content review and control, resulting in a decline in content quality and damage to information authenticity.

4.1.2 Misuse of big models to spread false information

Some bad elements abuse big computing models to spread false information, mislead the public and undermine social stability.

4.2 Specific Manifestations of Problematic Use Behavior

1) The quality of content is reduced and the authenticity of information is impaired. The content generated by over-reliance on large models often lacks depth and thinking, and the quality is not high. At the same time, because the training data of large models may be biased, the generated content may have the problem of information authenticity.
2) Users' blind trust in big models. Some users blindly trust the content generated by large models, lack the ability to distinguish information, and are easily misled by false information.
3) The impact on traditional media creation. The emergence of large computing models has had a certain impact on the creation of traditional media. Some traditional media practitioners may lose their jobs because of the competition of big models, and at the same time, the creative methods and values of traditional media may also be challenged.

4.3 The Potential Threat of Big Models to Digital Media Privacy

4.3.1 Increased risk of data leakage

Computing large models requires a large amount of data for training and optimization, which may contain personal information and privacy of users. If these data are leaked, it will have a serious impact on the rights and interests of users.

4.3.2 Potential for misuse of personal information

Computing big model can understand the user's interests, habits and other information by analyzing the user's data. If this information is abused, it will violate the privacy of users.

5 CONCLUSION

With the popularity and development of digital media, users' personal information and privacy are at increasing risk. At the same time, the problematic use behaviors of digital media have become increasingly serious, such as over-reliance on big models to generate content, and misuse of big models for false information dissemination, etc. These behaviors not only affect the quality of content and authenticity of information in digital media, but also pose a threat to the rights and interests of users and the stability of the society. Therefore, it is of great practical significance and urgency to study the privacy protection mechanism and problematic usage behaviors of digital media under computational big models. The privacy protection mechanism of digital media based on computational big model is a complex and important topic. The level of privacy protection in digital media can be effectively enhanced through the innovative application of encryption technology, the construction of intelligent defence systems, and the formulation and implementation of privacy protection policies. However, the existence of problematic usage behaviors still poses challenges to privacy protection. In the future, it is necessary to further strengthen technological innovation and policy regulation, as well as to raise public awareness of privacy protection, so as to jointly build a safe and trustworthy digital media environment.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This work is partially supported by 2023 Shenzhen Education Science Planning Project "Research on the Mechanisms and Strategies of Cross-border Co-operation in the Industry-Teaching Integration Community of Vocational Undergraduate Colleges and Universities (yb23048)", 2024 Guangdong Province Education Science Planning Project (Higher Education Special Project) "Research on Smart Classroom Teaching Behavior Analysis Methods Based on Scene Semantic Understanding and Deep Learning Characteristic Representation (2024GXJK766)", 2023 Guangdong Provincial Higher Vocational Education Teaching Reform Research and Practice Project "Research on Online Teaching Quality Evaluation Method Based on Multimodal Affective State Analysis (2023JG277)", 2024 Shenzhen Polytechnic University Quality Engineering Project "Research on Classroom Scene Understanding and Behavior Analysis Method Based on Multimodal Attention Mechanisms (7024310268)", 2024 Higher Education Scientific Research Planning Project of the Chinese Society of Higher Education "Research on the Analysis of Teaching and Learning Deep Interaction Characteristics in Smart Classroom Environment Supported by Multimodal Data (24XH0407)".

REFERENCES

[1] Spiekermann S. Viewpoint The Challenges of Privacy by Design.Communications of the ACM, 2012, 55(7): 38-40.

[2] Bélanger F, Crossler E R,Hiller S J, et al. POCKET: A tool for protecting children's privacy online. Decision Support Systems, 2013, 54(2): 1161-1173.

[3] Berendt B, Günther O, Spiekermann S. Privacy in e-commerce. Communications of the ACM, 2005, 48(4): 101-106.

[4] Degirmenci K. Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 2020, 50, 261-272.

[5] Spiekermann S. The challenges of privacy by design. Communications of the ACM, 2012, 55(7): 38-40.

[6] Spiekermann S, Acquisti A, Böhme R, et al. The challenges of personal data markets and privacy. Electronic Markets, 2015, 25(2): 161-167.

[7] Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. Science, 2015, 347(6221): 509-514.

[8] Neves J, Turel O, Oliveira T. Privacy concerns in social media use: A fear appeal intervention. International Journal of Information Management Data Insights, 2024, 4(2): 100260-100260.

[9] S. J H , Taylor J P, Kara B, et al. Digital Media and Developing Brains: Concerns and Opportunities. Current Addiction Reports, 2024, 11(2): 287-298.

[10] Ofir T, Hamed S Q, Isaac V. Special Issue: Dark Sides of Digitalization. International Journal of Electronic Commerce, 2021, 25(2): 127-135.

[11] Turel, Qahri-Saremi. Problematic Use of Social Networking Sites: Antecedents and Consequence from a Dual-System Theory Perspective. Journal of Management Information Systems, 2016, 33(4): 1087-1116.

[12] M S, M A M, A F, et al. Impact of a targeted direct marketing price promotion intervention (Buywell) on food-purchasing behaviour by low income consumers: a randomised controlled trial. Journal of human nutrition and dietetics: the official journal of the British Dietetic Association, 2017, 30(4): 524-533.

[13] Norman V, Ahlqvist M, Mattsson T. Evaluation of scale invariance in fatigue crack growth in metallic materials. International Journal of Fatigue, 2024, 189, 108545-108545.

[14] D'Ambrosio S, De Pasquale S, Iannone G, et al. Privacy as a proxy for Green Web browsing: Methodology and experimentation. Computer Networks, 2017, 126: 81-99.

[15] Ohme J, Araujo T, Boeschoten L, et al. Digital trace data collection for social media effects research: APIs, data donation, and (screen) tracking. Communication Methods and Measures, 2024, 18(2): 124-141.

[16] Dwivedi Y K, Ismagilova E, Hughes D L, et al. Setting the future of digital and social media marketing research: Perspectives and research propositions. International journal of information management, 2021, 59: 102168.

[17] Stoumpos A I, Kitsios F, Talias M A. Digital transformation in healthcare: technology acceptance and its applications. International journal of environmental research and public health, 2023, 20(4): 3407.

[18] Ahammed M F, Labu M R. Privacy-Preserving Data Sharing in Healthcare: Advances in Secure Multiparty Computation. Journal of Medical and Health Studies, 2024, 5(2): 37-47.

[19] Delaney J, Ghazi B, Harrison C, et al. Differentially Private Ad Conversion Measurement. Arxiv preprint arxiv: 2403. 15224, 2024.

[20] Jain P, Gyanchandani M, Khare N. Big data privacy: a technological perspective and review. Journal of Big Data, 2016, 3(1): 1-25.

[21] Imdad U, Roksana B, S S K. Privacy in targeted advertising on mobile devices: a survey. International journal of information security, 2022, 22(3): 31-32.

[22] Aridor G, Che Y K. Privacy Regulation and Targeted Advertising: Evidence from Apple's App Tracking Transparency. 2024.

[23] Borenstein B E, Taylor C R. The effects of targeted digital advertising on consumer welfare. Journal of Strategic Marketing, 2024, 32(3): 317-332.

[24] Ran H. Improved content recommendation algorithm integrating semantic information. Journal of Big Data, 2023, 10(1).

[25] Pan Y, Wang M, Lu L, et al. Scan-to-graph: Automatic generation and representation of highway geometric digital twins from point cloud data. Automation in Construction, 2024, 166, 105654-105654.

[26] J. M R. Signals and Images: Advances and Results in Speech, Estimation, Compression, Recognition, Filtering, and Processing. Photogrammetric Engineering & Remote Sensing, 2020, 86(2): 77-78.

[27] Bartoletti I, Plantié S, Sambodaran A. Security and privacy risks in the blockchain ecosystem. Cyber Security: A Peer-Reviewed Journal, 2019, 3(3): 195-207.

[28] Jia W, Guangbin W, Heng L, et al. Intelligent Construction Activity Identification for All-Weather Site Monitoring Using 4D Millimeter-Wave Technology. Journal of Construction Engineering and Management, 2024, 150(11).

[29] Zhu R, Srivastava A, Sutanto J. Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. Information Technology & People, 2020, 33(6): 1601-1626.

[30] Watson J, Lacey D, Kerr D, et al. Understanding the effects of compromise and misuse of personal details on older people. Australasian Journal of Information Systems, 2019, 23.
[31] Kani-Zabihi E, Helmhout M. Increasing service users' privacy awareness by introducing on-line interactive privacy features//Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011, Tallinn, Estonia, October 26-28, 2011, Revised Selected Papers 16. Springer Berlin Heidelberg, 2012: 131-148.
[32] Bilal A. Rise of technomoral virtues for artificial intelligence-based emerging technologies' users and producers: threats to personal information privacy, the privacy paradox, trust in emerging technologies, and virtue ethics. 2022.