Dokuz Eylül University Journal of Faculty of Business, Volume 25, Number 1, 2024, 111-130

Submission Date: March 1, 2024 Research Article
Acceptance Date: April 15, 2024 doi: 10.24889/ifede.1445367

Atıf/Citation:
Özdemir, K., Çelebi O. F. and Nacar, R. (2024). Consumer Security and Privacy In The Metaverse: A Bibliometric Analysis. *Dokuz Eylül University Journal of Faculty of Business*, 25(1): 111-130. https://doi.org/10.24889/ifede.1445367

CONSUMER SECURITY AND PRIVACY IN THE METAVERSE: A BIBLIOMETRIC ANALYSIS

Kadir ÖZDEMİR*, Ömer Faruk ÇELEBİ and Ramazan NACAR*****

ABSTRACT

The metaverse, one of today's most groundbreaking innovations, offers important opportunities for our future in many areas. However, these opportunities bring with them some critical threats. Security and privacy in the metaverse are among the most current threats that researchers focus on. Current studies that comprehensively analyze existing studies and develop solution suggestions for service providers and consumers in line with these analyses are pretty fragmented. Therefore, this study aims to provide a more concrete view and combine fragmented literature by using bibliometric techniques on security and privacy research in the metaverse in the WOS and SCOPUS databases. In addition, this study assesses the effects of the existing literature and offers a series of suggestions regarding measures that can be taken to protect consumer privacy and security. In the study, 86 studies published in 64 different sources between 2018 and 2024 are analyzed in terms of scientific performance with different bibliometric techniques. According to the prominent findings of the study, it is understood that the highest number of scientific publications were published in 2023; each publication received an average of 17 citations; single-author studies constitute 25% of all studies; and the most publications were published in the Journal of Metaverse. It is thought that the results revealed in this study and the suggested coping strategies regarding privacy and security will contribute to future studies. However, our proposed strategies for addressing privacy and security threats in the metaverse will provide guidance to service providers and consumers.

Keywords: Metaverse, Consumer Security, Consumer Privacy, Bibliometric Analysis, SPAR-4-SLR Protocol
JEL Classification: M10, M31, N7

METAVERSE'TE TÜKETİCİ GÜVENLİĞİ VE GİZLİLİĞİ: BİBLİYOMETRİK BİR ANALİZ

ÖZ

Günümüzün en çığır açıcı yeniliklerinden Metaverse, geleceğimiz için pek çok alanda önemli fırsatlar sunmaktadır. Ancak bu fırsatlar bazı kritik tehditleri de beraberinde getirmektedir. Metaverse'te güvenlik ve gizlilik araştırmacıların odaklandığı en güncel tehditler arasındadır. Mevcut çalışmaların kapsamlı bir analizini yapan ve bu analizler doğrultusunda hizmet sağlayıcılara ve tüketicilere yönelik çözüm önerileri geliştiren çalışmalar oldukça dağınıktır. Bu nedenle bu çalışma, WOS ve SCOPUS veri tabanlarında Metaverse'de güvenlik ve gizlilik araştırmaları üzerine bibliyometrik teknikler kullanarak daha somut bir görünüm sunmayı ve dağınık literatürü birleştirmeyi amaçlamaktadır. Ayrıca bu çalışma bir yandan mevcut literatürün etkinliğini değerlendirirken diğer yandan tüketici gizliliği ve güvenliğine karşı alınabilecek önlemlere ilişkin bir dizi öneriler sunmaktadır. Çalışmada 2018-2024 yılları arasında 64 farklı kaynakta yayınlanan 86 çalışma farklı bibliyometrik teknikler ile bilimsel performans bakımından analiz edilmektedir. Çalışmanın öne çıkan sonuçlarına göre en fazla bilimsel yayının 2023 yılında

* Research Assistant, Bursa Technical University, Faculty of Humanities and Social Sciences, Department of Business Administration, Bursa, Türkiye. E-mail: kadirozdemr3@gmail.com, https://orcid.org/ 0000-0002-2034-4797

** Research Assistant, Bursa Technical University, Faculty of Humanities and Social Sciences, Department of Business Administration, Bursa, Türkiye. E-mail: omer.celebi@btu.edu.tr, https://orcid.org/ 0000-0002-9462-6279

*** Prof., Bursa Technical University, Faculty of Humanities and Social Sciences, Department of Business Administration, Bursa, Türkiye. E-mail: ramazan.nacar@btu.edu.tr, https://orcid.org/ 0000-0002-4443-974X

üretildiği, her bir yayının ortalama 17 atıf aldığı, tek yazarlı çalışmaların tüm çalışmaların %25'ini oluşturduğu ve en fazla yayının Journal of Metaverse dergisinde yayınlandığı görülmektedir. Bu çalışmada ortaya çıkan sonuçlar ve gizlilik ile güvenliğe ilişkin önerilen stratejiler gelecek çalışmalara katkı sağlayacaktır. Bununla birlikte Metavers'te gizlilik ve güvenlik tehditlerine yönelik önerdiğimiz stratejilerin hizmet sağlayıcılar ve tüketicilere rehberlik edeceği düşünülmektedir.

Anahtar Kelimeler: Metaverse, Güvenlik, Gizlilik, Bibliyometrik Analiz, SPAR-4-SLR Protokolü
JEL Kodu: M10, M31, N7

1. INTRODUCTION

Innovative technologies transform and enrich our basic life practices, such as interaction and communication, day by day. Three significant transformations we have experienced have occurred through personal computers, internet access, and mobile phones, respectively (Mystakidis, 2022). Metaverse, representing the fourth wave of this transformation process, is seen as a new paradigm where individuals could experience the virtual world. It progresses depending on immersive technologies such as virtual reality (VR), augmented reality (AR) and emerging technologies like artificial intelligence (AI) and blockchain (Wang et al., 2022). Using AR and VR technology, Metaverse enables users to communicate and create value in virtual environments where the physical environment is simulated through avatars and holograms (Gursoy et al., 2022). The best-known examples of these environments are SecondLife, Fortnite, Roblox, and VR Chat (Dwivedi et al., 2023). Metaverse's utilization areas are not limited to gaming and communication platforms. On blockchain-supported metaverse platforms, users can freely carry out their financial activities according to the currency on the platform (Jeon et al., 2022). In addition, AI-supported metaverse is rapidly integrated into tourism (Buhalis et al., 2023) health, production, and smart cities (Huynh-The et al., 2023). On that sense, Metaverse is predicted to revolutionize many fields, from health to entertainment, marketing to tourism eventually (Hollensen & Opresnik, 2022).

According to Gartner, Metaverse is among the ten most strategic technology trends (Gartner, 2023). Aware of this trend, companies such as Facebook, Tencent, NVIDIA, and Microsoft have recently noticed their investments. The market is expected to enlarge further soon. It is estimated that the metaverse market, which has a global value of 47.8 billion dollars in 2022, will reach approximately 678 billion dollars in 2030 (Strategic Market Research, 2022). Since it is a newly adopted technology and is carried out with other technologies, the Metaverse must solve some problems to achieve its anticipated development (Chow et al., 2022). Security and privacy concerns of consumers are among the most critical problems hindering the development of the industry (Wang et al., 2022). Most of the security and privacy risks in Metaverse are similar to the threat's internet users are exposed to, such as malware, hacking attacks, identity theft and fraud, social engineering, phishing, surveillance, and tracking. However, due to its new structure, the Metaverse creates new threats, such as the exploitation of virtual assets and economies (Pooyandeh et al., 2022). Considering that Metaverse will gradually expand its sphere of influence, it is crucial for discuss both the current security-privacy risks and potential risks. In parallel with these developments, academic interest in the topic is growing. Previous studies, such as Wang et al. (2022), have explained the fundamentals of privacy and security threats in the metaverse, as well as the precautions that can be taken. According to Huang et al. (2023), the metaverse possesses four essential characteristics: socialization, real-world building, extensibility, and immersive interaction. Far and Rad (2022) described metaverse digital twin applications and security-privacy challenges, while Aks et al. (2022) discussed the use of blockchain for metaverse security. Kang et al. (2023) outlined the recommended security and privacy specifications for safe metaverse apps. Therefore, this study investigates all the current and potential security and privacy risks consumers face in Metaverse. In addition, the study aims to measure the effectiveness of publications in the current literature and identify research trends in related studies. Although these studies make unique contributions to the understanding of the subject, they indicate the need for a comprehensive study on privacy and security threats.

This study examined the current and potential security and risks of privacy that consumers face in the metaverse. Additionally, the study aims to assess the efficacy of publications in the current literature and to identify research trends in related studies through bibliometric findings. Existing research (e.g. Abbate et al., 2022; Wider et al., 2023; Rejeb et al., 2023; Feng et al., 2022; Shen et al., 2023; Chen & Zhang, 2022; Albahri & AlAmoudi, 2023; Bızel, 2023) have conducted bibliometric analyses of the metaverse. To our knowledge, no bibliometric research conducted on security and privacy issues in the metaverse. This study conducts bibliometric analysis according to the SPAR-4-SLR Protocol. Social science researchers frequently use the SPAR-4-SLR protocol in bibliometric analyses, systematic literature reviews, and meta-analyses. The most important contribution of this protocol to related methods is that it facilitates a repeatable, consistent, and transparent examination. Inconsistencies that may arise during the review process can be prevented through this protocol (Paul et al., 2021).

The following research questions will be addressed in this study to fill in any gaps in the literature:

RQ1: How have privacy and security issues in the metaverse evolved for academic researchers?

RQ2: What are the significant publications and authors that have contributed to research?

RQ3: Which areas of privacy and security in the metaverse are being researched currently and in the future?

The article is arranged as follows: General information about the metaverse's features and possible drawbacks is given in Section 2, while research design and methodology are covered in Section 3. Section 4 provides information on the findings and Section 5 discusses strategies for security in Metaverse, presents the popular examples of security risks in Metaverse and suggests general implications for individuals, institutions, and policymakers. It also provides suggestions for future research directions for interested researchers.

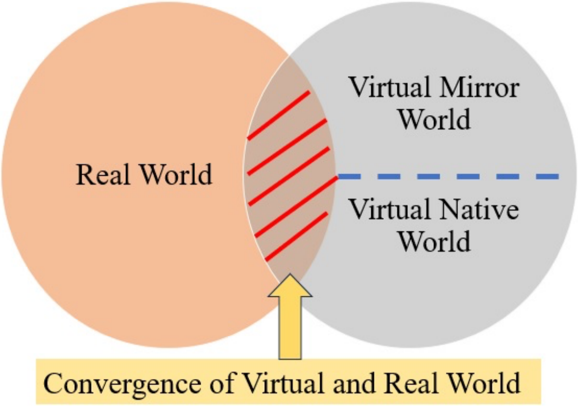
2. CONCEPTUAL BACKGROUND

2.1. The Metaverse: Overview and Challenges

The roots of the Metaverse term trace back to the dystopic novel "Snow Crash" by Stephenson, N. in 1992. However, it gained popularity when Zuckerberg introduced "Meta" as a new brand instead of Facebook in 2021 (Damar, 2021). Even though scholarly research has significantly increased, more consensus has yet to be reached on the definition of the Metaverse in the literature (Weinberger, 2022). Mystakidis (2022) describes the metaverse is a virtual world beyond reality that consists of digital virtuality and physical reality and includes many users. Otherwise, Huang et al. (2023) prefer a more straightforward definition: "the next-generation social world that everyone can access via the Internet."

Deloitte (2022) puts forward that this new-generation world consists of four elements: virtual mirror world, virtual native world, real world, and convergence of the real and virtual world. The connection among the elements of the Metaverse is presented in Figure 1. The first element of the Metaverse is the virtual mirror world, where business life, private life, and almost everything in the real world is simulated. The second element of the Metaverse is the virtual native world, which defines a space with different rules and possibilities from the real world. Bending some physical and spatial regulations in the real world offers significant opportunities (e.g., user creativity, free movement) for the virtual native world. That's why this space is critical in improving user skills in Metaverse. The real world is the third and most significant element of the Metaverse. Because the virtual world simulates the real world, and its value depends on interactions with the real world. The last element is the convergence of the virtual and real world. Soon, Metaverse will converge the real and virtual world. Thus, it is expected that interactions among the real and virtual world to increase (Deloitte, 2022) and this situation will create a kind of hybrid world eventually.

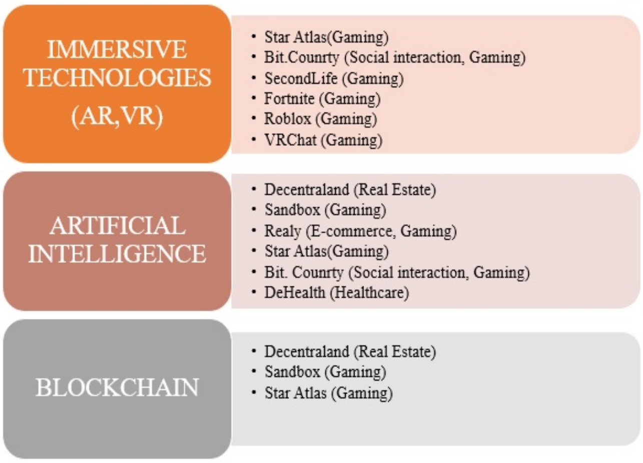
Figure 1: The Components of The Metaverse



Source: (Weinberger, 2022).

Metaverse is integrated with various technologies such as Edge Computing, Cloud Computing, Digital Twin, Network 5G, and 6G (Vladimirov et al., 2022). However, it progresses in its virtual adventure more through innovative AR, VR, AI, and Blockchain Technologies (Pooyandeh et al., 2022). Because these technologies get involved in Metaverse, many initiatives have emerged, from gaming to real estate and social interaction to healthcare (Huynh-The et al., 2023). Figure 2 shows Metaverse projects supported by these technologies. As seen in Figure 2, some projects (e.g., Decentraland, Sandbox, Star Atlas) include more than one technology. In addition, there are more examples of the gaming industry than other industries. Similarly, according to the last report by Strategic Market Research (2022), the gaming industry leads in the number of users adopting Metaverse.

Figure 2: Metaverse Projects Supported by Innovative Technologies



Source: Adapted from: (Dwivedi et al., 2023; Huynh-The et al., 2023).

Metaverse provides various opportunities for users. Its technology that allows virtual interaction can provide users with immersion and enhance their experience. For example, immersion offers a chance for a migrant living away from his family to feel the same emotional connection with his family in a virtual environment (Smaili & Rancourt-Raymond, 2022). In addition, it offers the opportunity to participate in concerts, touristic trips, and sports and art events via immersive technologies (Di Pietro & Cresci, 2021). Moreover, unique options are offered to users in finance, education, health, smart cities, and many other fields. Even though it expands in almost every area, serious security and privacy risks are barriers to users' adoption of it widely (Wang et al., 2022; Far & Rad, 2022). Because including various technologies in the Metaverse boosts novel threats that take time to resolve (Chow et al., 2022).

The Internet has introduced the terms security and privacy. However, in Metaverse, risks are more complex than on the Internet because Metaverse can process data in more detail than the Internet (Park & Kim, 2022). As with the Internet and other software systems, Metaverse has many security threats, such as malware and hacking attacks, identity theft and fraud, social engineering and phishing, exploitation of virtual assets and economies, surveillance, and tracking (Dwivedi et al., 2022; Chow et al., 2022; Awadallah et al., 2023). These threats will likely be in Metaverse as they can save all digital and virtual data (Benjamins et al., 2023).

2.2. Threats To Consumer Security in The Metaverse

One of the new concepts that emerged with the development of Metaverse is "Darkverse." Dwivedi et al. (2022) describe this term as the disadvantage of Metaverse and express that security threats are crucial among the disadvantages that must be considered. Metaverse users can be exposed to security threats in a variety of ways.

Malware and hacking attacks are one of the most common threats. Malware causes users' data to be obtained without their permission. So, there are risks that underage users could be forced to watch hazardous content (e.g., violence and pornography). Also, ransomware can cause economic exploitation of users. For example, there was a hacking attack on Roblox, and hackers demanded the game's virtual currency (Robux) as a ransom using ransomware (Dwivedi et al., 2023). Another threat that users are exposed to is identity theft and fraud. Data is more accessible to steal since users communicate in Metaverse via the avatar (Chow et al., 2022). In addition, with the recently developed Deepfake technology, users' biometric data can be counterfeited (Awadallah et al., 2023). Therefore, identity theft and fraud are critical threats that worry users and must be resolved.

Social engineering and phishing are other security threats to consider. Because there is so much social communication in the Metaverse, attacks of social engineering are possible to occur more intensely and frequently. These attacks are mainly carried out by manipulating the users' emotions, such as fear, curiosity, and panic. These manipulations cause victims' private information to be exploited for dangerous purposes (e.g., disclosure, exploitation of virtual assets and economies) (Di Pietro & Cresci, 2021; Huang et al., 2023).

Surveillance and tracking that makes users suspicious are among the potential threats on the dark sides. VR headsets and IoT devices mainly used in immersive technologies like AR and VR, have front-facing cameras. Although these are added to track the movement, they can capture many private data (e.g., biometric data, fields in the user's room). When attackers obtain these, they create surveillance and tracking threats for users (Chow et al., 2022; Dwivedi et al., 2022).

2.3. Safeguarding Privacy in The Metaverse

One of the most important topics of discussion in Metaverse is privacy. Protecting user's privacy is a fundamental human right. Thus, users' privacy expectations must be provided by laws, policies, particular details, and punishment-reward systems (Vladimirov et al., 2022; Gupta et al., 2023). Users may encounter unintended risks and dangers related to the privacy of individuals and businesses that desire to operate in it (Di Pietro & Cresci, 2021).

As in the internet environment users leave the digital crumbles behind that already tell a lot about tastes, habits, attitudes, emotions, personalities, and political and sexual orientations (Kosinski et al., 2013; Di Pietro & Cresci, 2021). For this reason, users are greatly concerned about this personal information and data collected. Users' privacy can be jeopardized unexpectedly (Falchuk et al., 2018). Indeed, data collection and analysis techniques in Metaverse are still in development. The platform can record the user's brainwaves, physiological responses, virtual and genuine environment interactions, and body movements. Especially, sensitive personal information that may leak through the Metaverse can include much real-world data about users (Di Pietro & Cresci, 2021). This phenomenon causes users to perceive risks and concerns about privacy. In this context, Metaverse can furnish undesirable odds for online deception, robbery, fraud, trickery, -stalking, and -bullying with the suffering of -attacks (Salahdine & Kaabouch, 2019; Vladimirov et al., 2022; Gupta et al., 2023).

Additionally, the identities of users/avatars may be illegally impersonated and stolen. In this situation, users' avatars, digital life and digital assets can be damaged, discredited, and even lost. With the -attacks in Metaverse, hackers may purloin banking details and full names (Zhao et al., 2022; Wang et al., 2022). For instance, in the Opensea NFT marketplace, the accounts of 17 users were hacked because of authentication loopholes, phishing attacks, and intelligent contract errors, which caused a loss of $1.7 million (Wang et al., 2022). To prevent such adverse and unpleasant events in Metaverse, laws or regulations are substantial to regulate users' behavior and adjust social relations. In this case, the literature highlighted three prominent principles that are briefly listed below (Almeida et al., 2021; Wang et al., 2022); respect human rights, being open, transparent, and consensus-driven, being publicly accountable.

Furthermore, although fundamental user privacy protection tools increase in Metaverse, users must learn or fully realize them (Fernandez & Hui, 2022). Examples of these tools are the Virginia Consumer Data Privacy Act, General Data Regulation Protection, Colorado Privacy Act, and the California Consumer Privacy Act which targets the preservation of individuals' data in virtual environments. These laws and regulations allow users to provide a homogeneous policy to protect their privacy (Fernandez & Hui, 2022; Nelson, 2023; De Haas et al., 2023).

3. METHODOLOGY AND RESEARCH DESIGN

This article applies bibliometric analysis techniques to the related literature to examine studies. This analysis is a quantitative method for obtaining measurable, repeatable and objective information from large amounts of bibliometric datasets (Ellegaard & Wallin, 2015). This method of analysis has become popular with the advent of scientific, which make it relatively easy to obtain large amounts of bibliometric data. Bibliometric analysis makes it possible to examine the development of an essential field of research, summarizing large amount of bibliometric data, revealing the intellectual structure of a research field and the status of emerging trends. It can also indicate future directions (Donthu et al., 2021).

In the literature, the SPAR-4-SLR protocol is frequently used for bibliometric analyses. Therefore, the methodological design of this study is based on the SPAR-4-SLR protocol. The protocol ensures accurate planning, consistency in execution and transparency to enable replication. The protocol also helps researchers to prevent problems and retain research integrity. The SPAR-4-SLR protocol consist of three main stages and six sub-stages. The steps of this research methodology and the phases of the SPAR-4-SLR protocol (Paul et al., 2021) are presented briefly in Table 1.

Table 1: SPAR-4-SLR Protocols

	Identification
Assembling	**Domain:** Security and privacy in the Metaverse **Research Questions:** See in introduction **Source Type:** Journal articles published and early access **Source Quality:** WOS and SCOPUS
	Acquisition
	Database: WOS and SCOPUS **Search Period:** Up to 17th January 2024 **Search Keywords**: (Privacy and Security) AND Metaverse Total Number of Articles Returned from the research: 288 WOS and 657 SCOPUS
Arranging	**Organization**
	Organizing Codes: Authors name, journal title, article title, countries, keywords, citation, coupling, networks

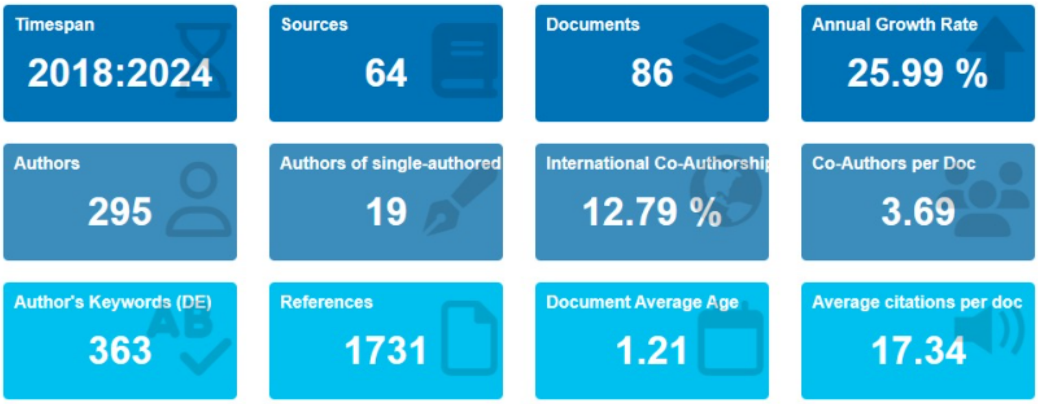
	Purification
	Document Type: Article **Subject Areas:** Social Sciences, Psychology, Business Management and Accounting
Assessing	**Evaluation**
	Analysis Method: Bibliometric analysis **Agenda Proposal Method:** Current research areas, keyword analysis, and recommendations for managing security and privacy threats in the Metaverse.
	Reporting
	Reporting Conventions: Tables, figures and words **Findings and Conclusion:** Theoretical and managerial implications **Limitation:** Database (WOS and SCOPUS), only English language

Many different software is used for bibliometric analysis, such as ScientoPyUI, Bibexcel, VOSviewer, CiteSpace, SciMAT and BiblioMaps. However, in this article, the bibliometric analysis was performed using Bibliometrix R, which is a valuable and efficient tool for visualization (Donthu et al., 2021).

4. FINDINGS

The following tables and figures illustrate the findings of the study.

Figure 3: Literature Overview



Timespan 2018:2024

Sources 64

Documents 86

Annual Growth Rate 25.99 %

Authors 295

Authors of single-authored 19

International Co-Authorshi 12.79 %

Co-Authors per Doc 3.69

Author's Keywords (DE) 363

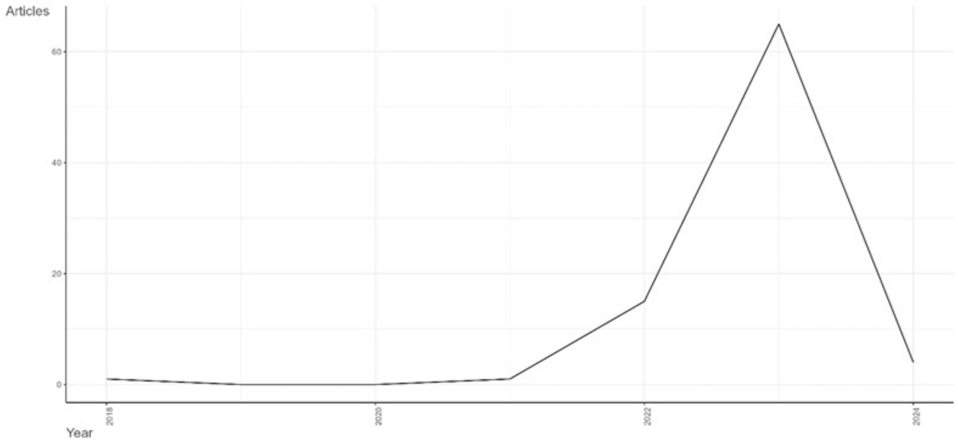
References 1731

Document Average Age 1.21

Average citations per doc 17.34

Figure 3 shows that the literature on privacy and security in the Metaverse is a relatively new field, with only 6 years of research resulting in 84 studies across 64 different sources. On average, each publication has around 17 citations. Approximately 25% of the studies were produced by a single author and international collaboration between authors was limited to about 13%.

Figure 4: Annual Scientific Production



There has been increasing interest in privacy and security in the metaverse since the first groundbreaking study on the subject was published in 2018 (Falchuk et al., 2018). 65 articles published in 2023 indicate that academic interest in this field will gradually increase.

Figure 5: Annual Citation Per Year

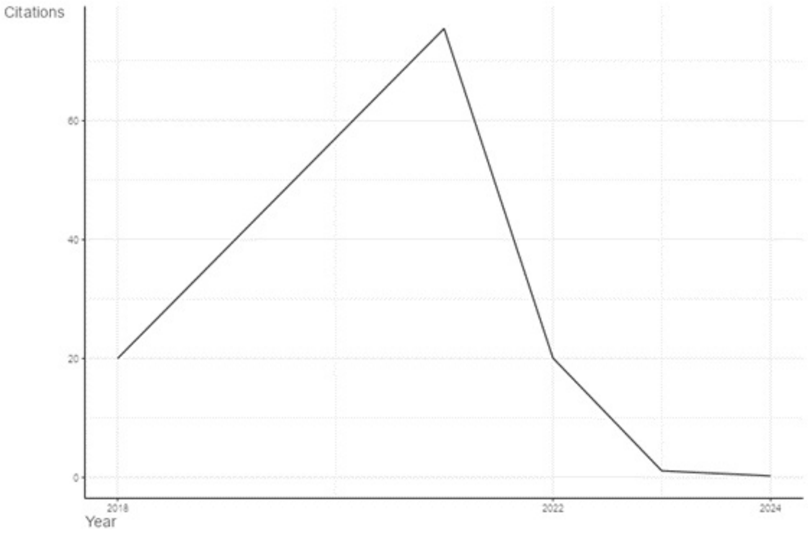


Figure 5 visualizes the annual citations per year. According to the Figure 5 the annual number of citations was approximately 20 in 2018, about tripled after 2020 and exceeded 60. As the number of studies increases, the number of citations is expected to increase.

Figure 6: Most Relevant Sources

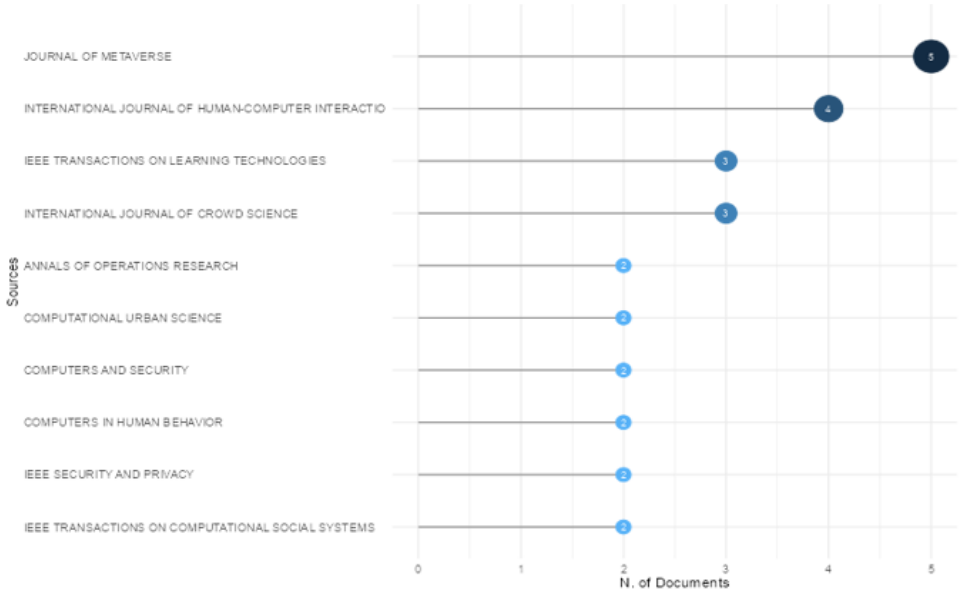


Figure 6 includes journals in which more than one study has been published. Accordingly, most studies published in the Journal of Metaverse. Although the journal only started publication in 2021, Metaverse has captured current and groundbreaking studies. The International Journal of Human-Computer-Interaction four, IEEE Transactions on Learning Technologies, and the International Journal of Crowd Science contributed to the literature by publishing three studies.

Figure 7: Most Relevant Authors

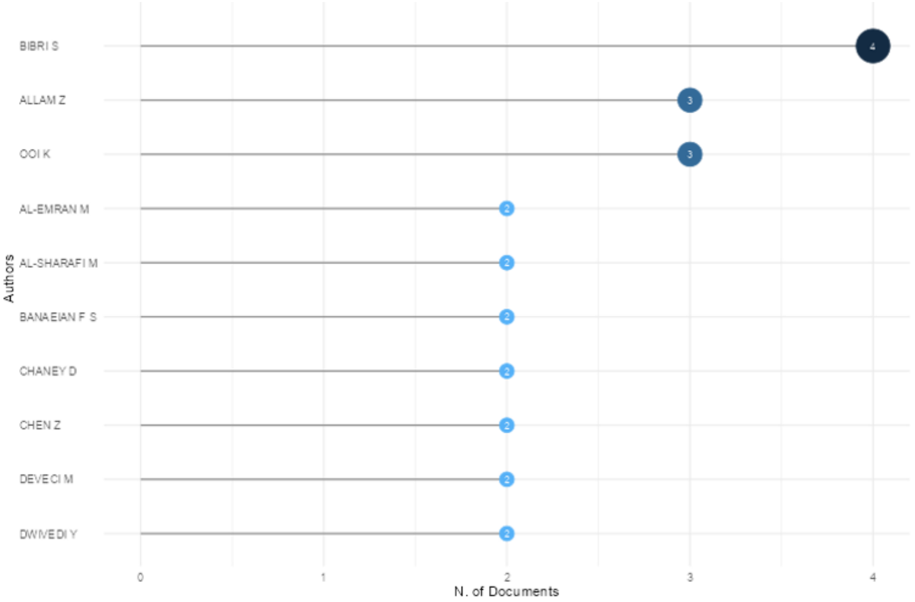
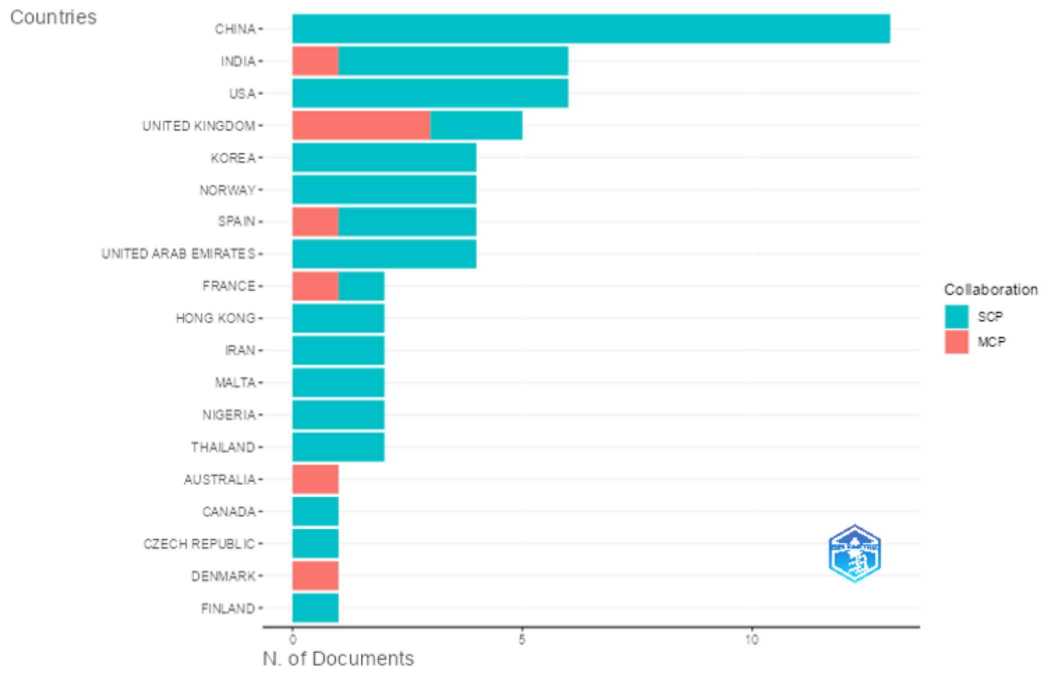


Figure 7 shares the information from the most relevant authors about the topic. The most contributing author is Simon Elias Bibri from École Polytechnique Fédérale de Lausanne. In his studies, Bibri emphasizes that the metaverse is an essential advantage for intelligent cities and discusses the measures to be taken against privacy and security threats (Bibri et al., 2022; Bibri & Allam, 2022). Another author who contributed the most to the subject is Zaheer Allam from Deakin University. Allam is also the co-author of many works by the most prolific writer, Bibri.

Figure 8: Corresponding Author's Countries



Note: SCP: Single Country Publication, **MCP:** Multiple Country Publication

Figure 8 shows the countries where the responsible authors publish in the field of metaverse security and privacy. China, India and the USA are the top countries for publishing. Although China is the leading country for publishing, there are no international collaborations. The UK leads in international collaborations. Given the dynamic nature of the topic, more international author collaborations are needed.

Figure 9: Co-occurrence Network

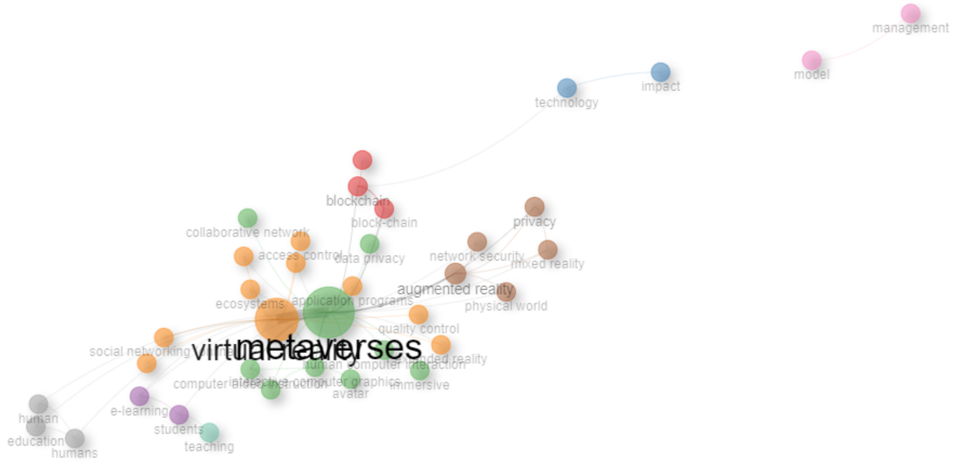
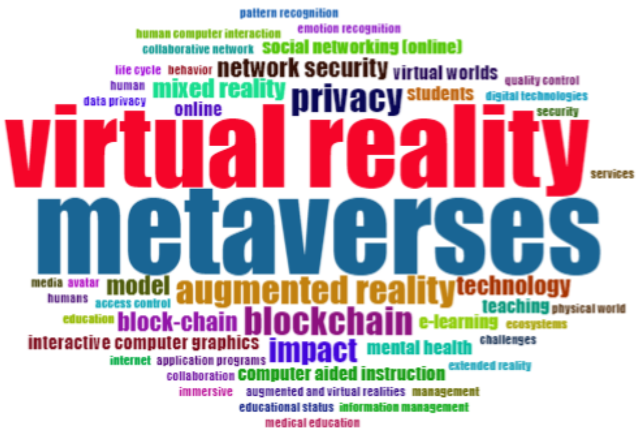


Figure 10: Word Cloud



Co-occurrence analysis is usually extracted from author keywords. This analysis assumes that there is a thematic correlation between words that appear together frequently. To predict and infer future research with noteworthy keywords, co-occurrence analysis of author keywords is used (Donthu et al., 2021). As shown in the Figure 9 and, Figure 10, the most common keywords are “metaverse”, “virtuality”, “augmented reality”, “data privacy”, “access control”, “physical world”, “privacy”, “network security”, “mixed reality”, “blockchain”, “collaborative network”, “technology”, “quality control”.

5. CONCLUSION AND DISCUSSION

The purpose of this study is to analyze the study of privacy and security in the metaverse by utilizing bibliometric analysis methods. We investigate current and potential security and privacy risks faced by consumers. Furthermore, we assess the effectiveness of current literature publications and identify research trends. The research comprises 84 studies from 64 diverse sources conducted over a period of six years. On average, each publication includes 17 citations. Single-authored studies account for 25% of the total, and international collaboration between authors was limited to approximately 13%. According to the results, most of the articles published in the Journal of Metaverse. This journal captured recent and groundbreaking studies, even though it only started publishing in 2021. Simon Elias Bibri from École Polytechnique Fédérale de Lausanne is the most contributing author. Another author who contributed significantly to the subject is Zaheer Allam from Deakin University. Allam has also co-authored many works with the prolific writer, Bibri. China is the leading country for publishing, however, there are no international collaborations. The highest number of international collaborations is in the UK. The co-occurrence analysis results indicate that 'metaverse', 'virtuality', 'augmented reality', 'data privacy', 'access control', 'physical world', 'privacy', 'network security', 'mixed reality', 'blockchain', 'collaborative network', 'technology', and 'quality control' are the most utilized keywords.

In conclusion, the emergence of the Metaverse brings forth a new wave of technological transformation, promising immersive experiences, and opportunities across various domains. However, the advancement and adoption of the Metaverse face crucial challenges, especially in the realms of consumer security and privacy. The potential risks and threats faced by users in the Metaverse are reminiscent of those encountered in traditional internet usage but are amplified due to the immersive nature and extensive collection of personal data in virtual environment. The evolving landscape of security and privacy in the Metaverse demands attention and proactive measures from stakeholders to safeguard user interests.

Various studies have highlighted the security threats in the Metaverse, including malware and hacking attacks, identity theft and fraud, social engineering and phishing, and surveillance and tracking. These threats can lead to the unauthorized access of personal information, economic exploitation, and manipulation of user experiences. (Dwivedi et al., 2023; Chow et al., 2022; Awadallah et al., 2023). Moreover, metaverse's extensive data collection capabilities also raise privacy concerns, users leave digital footprints that reveal personal information and preferences. The potential for online deception, fraud, -stalking, and -bullying raises concerns regarding users' safety and privacy (Salahdine & Kaabouch, 2019; Vladimirov et al., 2022; Gupta et al., 2023).

To address these challenges, stakeholders in the Metaverse ecosystem need to implement effective strategies for consumer security. One such strategy is the acceptance of a Zero Trust Architecture model, which emphasizes authentication, identity verification, data validation, access controls, and traffic validation (Gupta et al., 2023). By implementing the ZTA model, platform developers, service vendors, and device manufacturers can enhance the security of the Metaverse environment and protect user data.

Additionally, regulatory frameworks and privacy laws such as the Virginia Consumer Data Privacy Act, General Data Regulation Protection, Colorado Privacy Act, and the California Consumer Privacy Act play a crucial role in safeguarding user privacy in virtual environments (Fernandez & Hui, 2022; Nelson, 2023; De Haas et al., 2023). These regulations provide a standardized approach to privacy protection and give users with control over their personal information.

In summary, the Metaverse provide massive opportunities for users but also brings inherent risks to consumer security and privacy. It is essential for stakeholders to prioritize user protection, implement robust security measures like the ZTA model, and comply with relevant privacy regulations. By addressing these challenges and ensuring a safe and secure environment, the Metaverse can truly fulfill its potential as a transformative technological paradigm.

Future research in the marketing with a focus on consumer security and privacy within the Metaverse is crucial to provide the safeguard users' data and maintain trust in virtual environments. One key area for investigation is the development of effective privacy protection mechanisms within the Metaverse. Research could explore innovative approaches such as encryption, user authentication, and data anonymization techniques to safeguard personal information and mitigate privacy risks. Another important direction for future research is understanding consumers' perceptions and concerns regarding security and privacy in the Metaverse. Studying the factors that influence users' trust in virtual environments, their awareness of potential risks, and their willingness to engage in secure behaviors can provide valuable insights. This research could help marketers design strategies to communicate privacy practices effectively and build consumer confidence in the Metaverse. Moreover, exploring the impact of data breaches and security incidents on consumer trust and behavior within the Metaverse would be beneficial. Understanding how users react to such incidents, their expectations regarding transparency and accountability from companies, and their willingness to continue using virtual platforms can inform marketers' crisis management strategies and improve security measures. Lastly, considering the regulatory landscape surrounding security and privacy in the Metaverse is crucial. Future research could explore the implications of existing and emerging regulations on marketing practices, consumer protection, and data governance within virtual environments. Understanding the legal and ethical dimensions of marketing in the Metaverse will enable marketers to navigate potential challenges and ensure compliance with relevant laws and regulations. By addressing these future research directions, marketers can contribute to enhancing security and privacy measures in the Metaverse, fostering consumer trust, and promoting responsible marketing practices in virtual environments.

However, the findings of our study indicate that existing research is generally conducted in China, and international author collaborations remain limited. Therefore, future studies can consider different countries' contexts and turn to international author collaborations. Additionally, consumers' reactions in developed and developing country contexts to privacy and security threats in the metaverse can be examined comparatively.

The main contribution of this study is to reveal the scientific performance of the existing literature and coping strategies for privacy and security threats. Future studies can examine the relationships between consumer factors affecting privacy and security using the meta-analysis method. Additionally, through systematic literature reviews, consumers' responses to privacy and security threats can be addressed from theoretical, methodological, contextual, and characteristic perspectives. Finally, researchers can conduct experimental studies on consumers who experience the metaverse.

In addition to the contributions of this study, there are also some limitations. First, our study includes studies in the WOS and SCOPUS databases. This choice is because the WOS and SCOPUS databases index high-quality journals. Google Scholar and EBSCO databases, which contain studies of lower publication quality, were not included in the study. In this regard, our review may have missed some crucial studies in Google Scholar and EBSCO. Another limitation of our review is that it focuses on articles published in English. Some valuable studies conducted in different languages may not have been considered. Finally, our review is limited to the disciplines of "Business, Management, and Accounting," "Social Sciences," and "Psychology" in terms of subject matter. Therefore, we may have missed consumer security and privacy studies in different disciplines.

5.1. Strategies For Consumer Security in The Metaverse

As it is emphasized that one of the most crucial features of the Metaverse is security, as well as privacy, trust, and control. Some strategies can be conducted to ensure security (Far & Rad, 2022). All stakeholders such as platform developers, service vendors, and device manufacturers are responsible for these strategies. Zero Trust Architecture, a multi-party decentralized security model suitable for collaborative open environments, is known as one of these strategies. The ZTA model is depends on the "Don't trust, verify" logic and, is widely used to provide end-to-end security in virtual environments. Some of the substantial components in the ZTA model are authentication of everything, identity verification, data validation, access controls, traffic validation, and logs validations (Gupta et al., 2023).

Verification and user authentication are significant in the Metaverse because the face, video, and audio validation are used as digital avatars. With improved AR - VR tools and devices, hackers or attackers can easily imitate the same sounds and videos of users' appearance (Choi et al., 2022). One of the most critical challenges of virtual environments is providing anonymity which causes security and privacy issues and the spread of fake information and news (Chukwunonso et al., 2022). User/entity verification and authentication should be prerequisites in the Metaverse. Thus, the security and privacy issue will be solved by ensuring only pre-verification and authentication (Gupta et al., 2023; Choi et al., 2022). For instance, Twitter uses the "blue tick" symbol on selected profiles to indicate identity verification and authentication (Gupta et al., 2023).

In the metaverse, users might desire their identities to be visible, or they may also want to use digital avatars or twins to obtain a range of services. Creating a digital avatar or twin for users and mapping it to an encrypted database is the task of Identity Management (Gupta et al., 2023). Besides that, users often interact with and communicate with each other through digital avatars, and they only want the content of communication to be secret. A powerful solution to this object is encryption. The transmitter utilizes the key to encrypt the knowledge, and the receiver utilizes the correct key to decrypt the knowledge and receive the message. Thus, even if attackers get the ciphertext, they cannot decrypt and access the messages without the valid key (Zhao et al., 2022).

5.2. Best Practices for Privacy in The Metaverse

Blockchain technology, ensures data transparency, integrity, and resistance to tampering (Ryu et al., 2022), is used for decentralized cross-domain identity authentication for privacy. In the Metaverse environment, identity-based encryption and anonymous authentication protocols are used through the consortium blockchain to reduce security threats such as identity theft, privacy attacks, and extortion (Li et al., 2021; Choi et al., 2022). Another critical challenge in Metaverse is data-based transaction attacks. To deal with this challenge, hash-chain-based aggregate digital signature techniques are used. Developed threat detection methods depends on multi-factor authentication and robust password techniques are also used (Choi et al., 2022).

Quantum Random Number Generation and Quantum Key Distribution techniques are used to enhance the service quality and security of the Metaverse. Quantum techniques are also used for optimization, computation, randomness, and communication in the Metaverse (Azzaoui et al., 2021). Elliptic Curve Cryptography (ECC) is also widely used as a privacy practice. ECC uses an elliptic curve over an extensive finite area, ensuring better security and privacy execution with significantly smaller key sizes than current essential cryptography techniques. Another practice used for privacy and security is Biohashing. With this method, the biometric data, such as fingerprints of the users, is used as an additional security factor. Also, the Dolev-Yao (DY) model, frequently used for private practice, is about protocol privacy and security. In addition to that, the Canetti-Krawczyk (CK) model, an advanced version of the DY model, is used (Ryu et al., 2022).

In Metaverse, big data that increases competition, productivity, innovation, and creativity and allows businesses to offer novel values is quickly collected, processed, and analyzed. The data given by Metaverse is much more worthful than the data obtained from typical 2D social media platforms. However, one of the challenges of Metaverse is user profiling depends on the large amount of data collected. For this reason, ethical considerations are extensively significant in all virtual environments and digital platforms (Anshari et al., 2022). For example, Facebook conducted a secret mood experiment called emotional contagion with researchers at Cornell University to provide insight. In this research, the private data of Facebook users were used. During the data mining process, they did not receive explicit approval about whether users desired to participate in the research. When Facebook shared the results of its investigation, it received lots of negative feedback, and this research was found unethical (Fishwick, 2014; Meyer, 2014). The platform providers are committed to guarantee the privacy and security. It is a fact that has not yet solved serious issues that must be considered. One of these issues is that attackers obtain private data without users' permission. The other problem is whether platform providers have the power to intercept it or not. It is unethical to violate an individual’s private life and human rights without permission. Even if users allow their data to be used, businesses should not be allowed to use it to maximize their profits (Anshari et al., 2022).

REFERENCES

Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., & Riccio, E. (2022). A first bibliometric literature review on Metaverse. *In 2022 IEEE Technology and Engineering Management Conference (TEMSCON EUROPE)*, 254-260, IEEE.

Aks, S. M. Y., Karmila, M., Givan, B., Hendratna, G., Setiawan, H. S., Putra, A. S., ... & Herawaty, M. T. (2022). A Review of Blockchain for Security Data Privacy with Metaverse. In 2022 International Conference on ICT for Smart Society (ICISS), 1-5, IEEE.

Albahri, O. S., & AlAmoodi, A. H. (2023). Navigating the Metaverse of Big Data: A Bibliometric Journey. Mesopotamian Journal of Big Data, 92-106.

Almeida, V., Filgueiras, F., & Doneda, D. (2021). The ecosystem of digital content governance. *IEEE Internet Computing,* 25(3), 13-17.

Anshari, M., Syafrudin, M., Fitriyani, N. L., & Razzaq, A. (2022). Ethical Responsibility and Sustainability (ERS) Development in a Metaverse Business Model. *Sustainability*, 14(23), 15805.

Awadallah, A. M., Damiani, E., Zemerly, J., & Yeun, C. Y. (2023). Identity Threats in the Metaverse and Future Research Opportunities. *In 2023 International Conference on Business Analytics for Technology and Security (ICBATS)* 1-6, IEEE.

Azzaoui, A. E., Kim, T. W., Pan, Y., & Park, J. H. (2021). A quantum approximate optimization algorithm based on blockchain heuristic approach for scalable and secure smart logistics systems. Human-centric Computing and Information Sciences, 11(1).

Benjamins, R., Rubio Viñuela, Y., & Alonso, C. (2023). Social and ethical challenges of the metaverse: Opening the debate. *AI and Ethics*, 1-9.

Bızel, G. (2023). A bibliometric analysis: Metaverse in education concept. *Journal of Metaverse*, 3(2), 133-143.

Bibri, S. E., Allam, Z., & Krogstie, J. (2022). The Metaverse as a virtual form of data-driven smart urbanism: platformization and its underlying processes, institutional dimensions, and disruptive impacts. *Computational Urban Science,* 2(1), 24.

Bibri, S. E., & Allam, Z. (2022). The Metaverse as a virtual form of data-driven smart cities: The ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society. *Computational Urban Science*, 2(1), 22.

Buhalis, D., Leung, D., & Lin, M. (2023). Metaverse as a disruptive technology revolutionising tourism management and marketing. *Tourism Management*, *97*, 104724.

Chen, D., & Zhang, R. (2022). Exploring research trends of emerging technologies in health metaverse: A bibliometric analysis. *SSRN, 1-32.*

Choi, M., Azzaoui, A. E., Singh, S. K., Salim, M. M., Jeremiah, S. R., & Park, J. H. (2022). The Future of Metaverse: Security Issues, Requirements, and Solutions. Human-Centric *Computing and Information Sciences*, 12.

Chow, Y. W., Susilo, W., Li, Y., Li, N., & Nguyen, C. (2022). Visualization and Cybersecurity in the Metaverse: A Survey. *Journal of Imaging*, 9(1), 11.

Chukwunonso, A. G., Njoku, J. N., Lee, J. M., & Kim, D. S. (2022). Security in metaverse: a closer look. *In Proceedings of the Korean Telecommunications Society Conference*, Seoul, South Korea, 9-11.

Damar, M. (2021). Metaverse shape of your life for future: A bibliometric snapshot. *Journal of Metaverse*, 1(1), 1-8.

De Haas, E., Yiming, H., Bermejo, C., Lin, Z., Hui, P., & Lee, L. H. (2023). Towards Trustworthy Augmented Reality in The Metaverse Era: Probing Manipulative Designs in Virtual-Physical Commercial Platforms. *In 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, 779-780. IEEE.

Deloitte, (2022). *The Metaverse Overview Vision, Technology, and Tactics.* https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/metaverse-report.html. Date of Access: 08.12.2023.

Di Pietro, R., & Cresci, S. (2021). Metaverse: security and privacy issues. *In 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 281-288, IEEE.

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.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 102542.

Dwivedi, Y. K., Hughes, L., Wang, Y., Alalwan, A. A., Ahn, S. J., Balakrishnan, J., ... & Wirtz, J. (2023). Metaverse marketing: How the metaverse will shape the future of consumer research and practice. *Psychology & Marketing*, *40*(4), 750-776.

Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact?. *Scientometrics*, 105, 1809-1831.

Falchuk, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. *IEEE Technology and Society Magazine*, 37(2), 52-61.

Far, S. B., & Rad, A. I. (2022). Applying digital twins in metaverse: User interface, security and privacy challenges. *Journal of Metaverse*, 2(1), 8-15.

Feng, X., Wang, X., & Su, Y. (2022). An analysis of the current status of metaverse research based on bibliometrics. *Library Hi Tech*.

Fernandez, C. B., & Hui, P. (2022). Life, the Metaverse and everything: An overview of privacy, ethics, and governance in Metaverse. *In 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 272-277, IEEE.

Fishwick, C. (2014). *Facebook's secret mood experiment: have you lost trust in the social network?*. https://www.theguardian.com/technology/poll/2014/jun/30/facebook-secret-mood-experiment-social-network. Date of access: 12.06.2023.

Gartner, (2023). *Top Strategic Technology Trends 2023*. https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/2023-gartner-top-strategic-technology-trends-ebook.pdf. Date of Access: 10.12.2023.

Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., & Shabaz, M. (2023). Metaverse Security: Issues, Challenges and a Viable ZTA Model. *Electronics,* 12(2), 391.

Gursoy, D., Malodia, S., & Dhir, A. (2022). The metaverse in the hospitality and tourism industry: An overview of current trends and future research directions. *Journal of Hospitality Marketing & Management*, 31(5), 527-534.

Hollensen, S., Kotler, P., & Opresnik, M. O. (2022). Metaverse–the new marketing universe. *Journal of Business Strategy*, 44(3), 119-125.

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, 6(2), 234-247.

Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2023). Artificial intelligence for the metaverse: A survey. *Engineering Applications of Artificial Intelligence*, 117, 105581.

Jeon, H. J., Youn, H. C., Ko, S. M., & Kim, T. H. (2022). Blockchain and AI Meet in the Metaverse. *Advances in the Convergence of Blockchain and Artificial Intelligence*, 73(10.5772).

Kang, G., Koo, J., & Kim, Y. G. (2023). Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective, *IEEE Communications Magazine*.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110(15), 5802-5805.

Li, M., Weng, J., Liu, J. N., Lin, X., & Obimbo, C. (2021). Toward vehicular digital forensics from decentralized trust: An accountable, privacy-preserving, and secure realization. *IEEE Internet of Things Journal*, 9(9), 7009-7024.

Meyer, R. (2014). *Everything We Know About Facebook's Secret Mood-Manipulation Experiment.* https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/. Date of access: 12.06.2023.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, 2(1), 486-497.

Nelson, W. (2023). Navigating state data privacy laws: A guide for SEC-registered investment advisers. *Journal of Financial Compliance*, 6(3), 281-290.

Park, S., & Kim, S. (2022). Identifying world types to deliver gameful experiences for sustainable learning in the metaverse. *Sustainability*, 14(3), 1361.

Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, 45 (4), 1-16.

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences*, 12(24), 12993.

Rejeb, A., Rejeb, K., & Treiblmaier, H. (2023). Mapping Metaverse Research: Identifying Future Research Areas Based on Bibliometric and Topic Modeling Techniques. *Information*, 14(7), 356.

Ryu, J., Son, S., Lee, J., Park, Y., & Park, Y. (2022). Design of secure mutual authentication scheme for metaverse environments using blockchain. *IEEE Access*, 10, 98944-98958.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, 11(4), 89.

Shen, J., Zhou, X., Wu, W., Wang, L., & Chen, Z. (2023). Worldwide Overview and Country Differences in Metaverse Research: A Bibliometric Analysis. *Sustainability*, 15(4), 3541.

Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: welcome to the new fraud marketplace. *Journal of Financial Crime*, 31(1), 188-200.

Strategic Market Research, (2022). *Metaverse: A New Digital World (Statistics & Facts).* https://www.strategicmarketresearch.com/blogs/metaverse-statistics. Date of Access: 09.12.2023.

Stephenson, N. (1992). Snow crash. Penguin Books.

Vladimirov, I., Nenova, M., Nikolova, D., & Terneva, Z. (2022). Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey. *In 2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, 1-4, IEEE.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, *25*(1), 319-352.

Weinberger, M. (2022). What Is Metaverse? - A Definition Based on Qualitative Meta-Synthesis. *Future Internet*, 14(11), 310.

Wider, W., Jiang, L., Lin, J., Fauzi, M. A., Li, J., & Chan, C. K. (2023). Metaverse chronicles: a bibliometric analysis of its evolving landscape. *International Journal of Human–Computer Interaction*, 1-14.

Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2022). Metaverse: Security and privacy concerns. *Journal of Metaverse*, 3(2), 93-99.