REVIEW ARTICLE

Virtual Tourism Cybersecurity: A Scientometric Analysis of Research Trends

Naveen Bhamasi[1], **Garima Thakur**[1], **Sunil Prajapat**[2,*] **and Pankaj Kumar**[1]

[1] Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala 176215, India
[2] Department of Computer Engineering AI and Big Data, Marwadi University, Rajkot 360003, India

Abstract

The rapid pace of technological developments in the digital age has transformed the tourism sector, spawning virtual tourism, an emerging platform through which tourists are able to visit their destination using augmented reality (AR) and virtual reality (VR) for interactive experiences. Such technological transformation creates significant cybersecurity challenges, such as data breaches, violations of users' privacy, and vulnerabilities on platforms. Therefore, our work uses bibliometric approaches to examine the growing body of research on virtual tourism cybersecurity. A total of 1145 publications were retrieved using the specified query, which includes studies on the dangers of data theft, malware threats, shoddy authentication procedures, and improper usage of augmented and virtual reality technologies. Our investigation identifies leading cybersecurity academics, top publications, primary research clusters, and regional research bases. Cybersecurity research on virtual tourism helps academics create better security methods by highlighting areas of the subject that are explored less. Consequently, the scientific results of this study give decision-makers in the fields of virtual tourism development and web security the ability to create more reliable and effective systems for users.

Keywords: cybersecurity, virtual tourism, scientometric, scopus data, virtual reality.

1 Introduction

Virtual tourism has risen as a significant innovation in the sphere of the travel industry, providing users with the ability to explore destinations via advanced technologies like virtual reality and augmented reality. VR creates fully immersive digital environments where users can interact with a simulated world using headsets and motion sensors, effectively transporting them to virtual destinations. AR, on the other hand, recreates the physical environment with the interactive overlaying of digital elements onto the real world using different software like the Measure app on iPhone and some devices like smartphones or AR glasses. These technological platforms create sustainable interactive travel solutions that minimize environmental impact while increasing accessibility to destinations. Growing environmental concerns and the need for global accessibility lead to the rise of virtual tourism. Virtual tourism serves as a sustainable option by reducing

Submitted: 23 October 2025
Accepted: 01 December 2025
Published: 20 December 2025

Vol. 1, **No.** 1, 2025.
10.62762/JRSC.2025.547593

***Corresponding author:**
✉Sunil Prajapat
sunilprajapat645@gmail.com

Citation
Bhamasi, N., Thakur, G., Prajapat, S., & Kumar, P. (2025). Virtual Tourism Cybersecurity: A Scientometric Analysis of Research Trends. *Journal of Reliable and Secure Computing*, 1(1), 41–53.

© 2025 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

carbon emissions linked with traditional travel and allows people with mobility limitations or financial constraints to experience distant destinations [1, 2]. As environmental concerns rise among travelers, the adoption of virtual platforms has accelerated, reflecting a shift toward responsible and inclusive tourism practices, [3, 4].

However, this rapid growth exposes users to a wide range of cybersecurity threats, jeopardizing their privacy, data security, and platform dependability. Users typically use platforms that require sharing sensitive personal data, such as full names, email addresses, and payment card details, to access premium virtual tours or purchase digital souvenirs. These transactions usually occur over open networks where unauthorized entities can easily intercept data in transmission [5]. For instance, a user books a virtual tour of a mountain summit place from an AR-based tourism app. When a user agrees to the booking, the platform asks for personal information along with the credit card details. This data is sent through a public channel. Without strong security measures such as end-to-end encryption, cybercriminals could perform several attacks like man-in-the-middle (MITM), impersonation, etc., to capture user data, which results in different types of fraud or identity theft.

Therefore, it is crucial to implement robust cybersecurity strategies specifically tailored for virtual tourism environments to mitigate these risks. These involve implementing blockchain to carry out secure transactions, using AI-based intrusion detection systems, and engaging encrypted channels for communications. In addition to compliance with data protection regulations such as GDPR (General Data Protection Regulation), virtual tourism ensures responsible collection, storage, and processing of visitors' personal data. Since virtual tourism platforms use technologies like VR, AR, and AI to collect data like name, location, preferences, and even biometric data, GDPR plays a key role in protecting user privacy; it also makes users' privacy and the platforms more reliable and regulated [6]. Artificial intelligence (AI) improves customer engagements through predictive analytics and better customer service but opens up users to risks from both adversarial threats and data privacy. Increasing reliance on public networks, flawed modes of authentication, and non-standardized cybersecurity measures by platforms and across silos further compound the challenge of cybersecurity.

Indeed,"The study on cybersecurity matters in virtual tourism through scientometric analysis," we can establish "greater homogeneity in reviews of research trends," we can find "vacant spaces to develop security solutions for this sector," and at the same time, it forms an "important methodology to study the academic knowledge structure" of cybersecurity research in virtual tourism. Bibliometric data, which is analyzed on publication statistics about the trajectory of research mapping from the view standings towards an exploratory overview of the entire academic domain, helps in placing the leading authors, institutions, influential journals, and prevailing keywords that bring the research progress of the field to light. The geographic distribution of research activity informs how different regions are engaging with cybersecurity challenges and concerns in virtual tourism [7].

2 Literature Review

The cybersecurity and virtual tourism crossover has received more and more academic attention due to the rapid growth of AR/VR technologies and their inherent vulnerabilities within the platforms. Some studies have tried to uncover potential threats and discuss data privacy issues on technologies alongside other possible technological measures to counter the issues.

Anwar et al. [8] also drew limelight into the susceptibility of AR/VR systems involved in virtual tourism to various forms of cyberattacks, added but not limited to malware, ransomware, and unauthorized access to user data. If robust encryption protocols during data transmission are not available, attacks like man-in-the-middle (MITM) and personal as well as financial data become vulnerable to interception. In a related context, Ampountolas et al. [9] mentions the sudden adoption of AR/VR platforms before proper security measures were implemented; hence, virtual tourism platforms have no protection against breaches. Users' information, which includes login details, location, and payment information, is at stake since there are no adequate methods of authentication. Furthermore, Kovačić et al. [10] pinpointed cybersecurity's relationship with users' trust and, thus, with platform sustainability. Data breaches are often reported, along with security vulnerabilities that had not been addressed. These all, in turn, reduce consumer confidence in virtual tourism services and hence tend to retard the development of this industry. That study gave more information on how to use AI-driven intrusion detection systems

and real-time threat monitoring to make cybersecurity stronger. Bhattacharya et al. [28] conducted a regulatory discussion, challenging policies and laws in the AR/VR cybersecurity environment. Fragmentation in the cybersecurity frameworks, findings point out, stands as the single most enormous business barrier. The absence of common data protection regulations leaves virtual tourism platforms exposed. Therefore, Huang suggests developing unified legal frameworks to overcome the challenges and spearhead international collaboration on cybersecurity strategies.

Phishing attacks, a major topic in the landscape of virtual tourism, have been discussed by Saeed et al. [11]. The research has established that frail authentication behavior, accompanied by a lack of cybersecurity risk knowledge from users, provides leverage to cybercriminals in exploiting virtual tourism networks. Attacks are majorly centered around the public WiFi network from where the tourists access AR/VR travel services, further escalating all conditions for data theft. Sinha et al. [12], in their study, confirmed these results, stating that the many vulnerabilities in public networks increase the risk of illegal monitoring and interception of information. Hence, the study put more emphasis on the urgency of creating secure network connections and using multi-factor authentication mechanisms that can be applied to protect the information of the user. Blockchain technology has also come up as a potential healthy remedy for cybersecurity in virtual tourism. Calvaresi et al. [13] has evaluated the role of blockchain to decentralize data storage, maintain data integrity, and trigger aggregated data breaches in the practical study of blockchain imperfection. While promising security enhancements, Bogicevic [13] also acknowledged persistent issues of scalability and high energy consumption. Optimization needs to be triggered more and more.

Collectively, the literature once again underlines the pressing need to respond to cybersecurity risks for virtual tourism. Whether various aspects have already been critiqued, such as vulnerabilities to AR/VR attacks, phishing strikes, legal cracks, and blockchain-centered security, something very important is missing until now: adaptive security modeling, user education, and global cybersecurity standards to be further researched.

3 Objectives

- The study focuses on discovering the leading keywords that appear in research about cybersecurity matters in virtual tourism.
- The evaluation measures the documents' impact through citation analysis.
- The research aims to evaluate the citation impact made by individual authors working in this field.
- The co-authorship relationships between scientists in this subject area will be investigated.

4 Significance

Tourism has witnessed the rapid implementation of digital technologies resulting in virtual tourism platforms that present new cybersecurity risks. During the COVID-19 pandemic, virtual tourism gained importance as a vital sector of tourism operations because it allows travelers to virtually visit locations through digital virtual spaces. Virtual tourism, enabled by the accelerated development of virtual reality (VR) and augmented reality (AR) and other immersive systems, opens new exciting possibilities yet creates essential security obstacles.

The development and assessment of a research field depend on scientometric analysis, which employs quantitative approaches to investigate cybersecurity trends and study impact within virtual tourism environments. Scientometric methods to analyze academic data about research publications coupled with citations help reveal patterns while locating essential research sectors and demonstrating how cybersecurity risks transform over time inside virtual tourism. Virtual tourism security research can receive focused attention through this kind of analysis, which reveals important system vulnerabilities, particularly data breaches and user privacy violations and attacks against VR/AR platforms [14].

Scientometric analysis offers policymakers, alongside cybersecurity experts and technology developers, valuable knowledge about the depth and extent of virtual tourism cybersecurity problems. The analysis indicates which security issues need immediate focus, including the protection of virtual environment data security and payment system development for virtual tourism. The study of influential publications and citation networks allows researchers to identify peers leading cybersecurity in virtual tourism platforms so they can promote collaboration while developing security standards [15].

Guidance for future research directions emerges from scientometric analysis. This analysis discovers unaddressed literature gaps showing the necessity

for point-of-interest examinations about cyber threats within virtual tourism and security solution investigations for evolving virtual environments. The evolution of virtual tourism requires an apex level of scientometric analysis to build resilient cybersecurity strategies for defending users while protecting touristic sites and businesses against cyberthreats [16, 17].

The advancing importance of cybersecurity protection in virtual tourism goes beyond theoretical discussions because it affects tourism businesses directly by depending heavily on customer trust relations. Virtual tourism platforms handle sensitive information, including personal details and payment data, which endures financial consequences and damages reputation when security breaches occur for the tourism sector's companies. Scientific research analysis of industries' behavioral patterns alongside security risks and preventive approaches enables sustained development of this industry, yet it maintains its growth while combating threats.

The results of this scientometric analysis are expected to serve as a foundation for future research, enabling more secure and resilient virtual tourism ecosystems. By bridging academic inquiry with practical application, the study aims to make a lasting impact on this rapidly evolving field.

5 Research Methodology

This research examines existing literature on virtual tourism cybersecurity issues by utilizing a scientometric analysis method. Scientists apply a systematic assessment of publications combined with citation analysis to evaluate the knowledge structure and pattern formation within this specific domain.

1. **Data Collection.**
   (a) Select a database to perform the research.
   (b) Searching and gathering domain-specific literature with the help of a well-compiled search query.
   (c) Manual review of the database, where the data is filtered according to time, language, and subject area.
2. **Processing and visualization tool.** Choosing a visualization tool.
3. **Data analysis.** Identifying and interpreting the results.

5.1 Data Selection

Data can be collected by using various databases like Scopus, Web of Science, Google Scholar and Research Gate. Google Scholar covers books content along with other freely accessible online publications, while Scopus and Web of Science focus more on scholarly information. The majority of the papers that were studied came from the Scopus database which is a large citation database that contains broad and influential articles. The following retrieval code was used in the Scopus database: total of 1144 documents were retrieved.

The related papers were identified when the defined terms appeared in the title, or keywords, or abstracts, which ensure that the data is as comprehensive as possible. After collection of the data, it was downloaded.

5.2 Processing and Visualization tool

The user-friendly adjustment capabilities of VOSviewer enable researchers to explore bibliometric networks, including co-authorship relationships, co-citation patterns, and keyword clusters. Biblioshiny for R is preferred for its combination of interactive dashboard functionality and advanced bibliometric analysis, all with minimal programming effort. Gephi allows users to create visual representations of complex network dynamics by constructing custom views that reveal intricate co-author connections. Research papers were analyzed primarily with VOSviewer software as the main analysis tool.

5.3 Data Analysis

A cluster analysis approach enabled the review to organize research themes. Cluster analysis stands as a popular method in statistical data analysis within the studied domain. Then, three scientometric techniques were performed as following:

1. *Co-author analysis:* The author and country co-occurrence network forms an integral part of this analysis.
2. *Co-words analysis:* This part analyzes both keyword co-occurrence network structures in combination with keyword evolution network models.
3. *Critical Review:* The research team completed a critical analysis to reveal themes while understanding associated research difficulties.

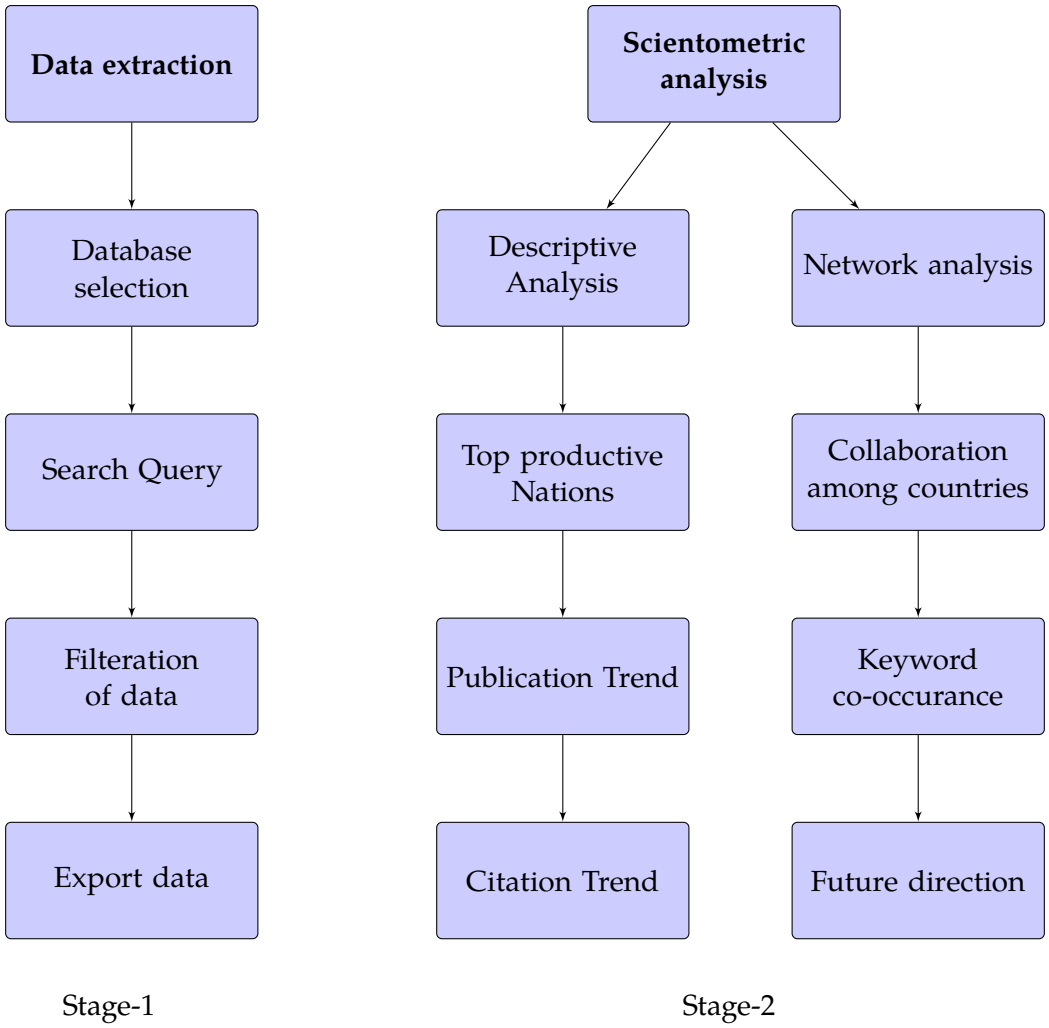

Figure 1. Schematic overview of the research methodology, illustrating the two-stage process: data extraction (Stage-1) and the subsequent descriptive and network-based scientometric analysis (Stage-2).

The complete process is shown in Figure 1 using pictorial representation

6 Results

6.1 Co-Occurrence Analysis of all Keywords

A comprehensive co-occurrence analysis examined how terms and their associations work together at the intersection of cybersecurity issues in virtual tourism. This analysis revealed important thematic patterns which helped understand research directions. The extracted keywords were analyzed with VOSviewer and Biblioshiny for R to create visual presentations that showed how various keywords related to each other. The analysis identified clusters of related keywords that showcase dominant research areas including "virtual tourism security" and "data protection" alongside "smart tourism ecosystems" and "cybersecurity strategies." The examination of co-occurring patterns found current research trends combined with existing study gaps to provide direction for additional research in this field. The frequency of occurrence and total link strength of the prominent keywords are summarized in Table 1.

To find important relationships in our dataset of 5,270 keywords we performed a co-occurrence analysis. Our analysis included only keywords that showed up at least five times to gather meaningful results. Our study used 247 keywords that met a minimum count threshold to find useful connections between terms. We exclude unnecessary data terms to refine our examination of key relationships and patterns. By analyzing 247 main keywords the analysis finds important patterns showing how subjects relate to each other. When keywords show up together in research content we can see which words relate to and connect with each other. This method shows how strongly keywords connect to each other while showing how often they appear together. The resulting keyword

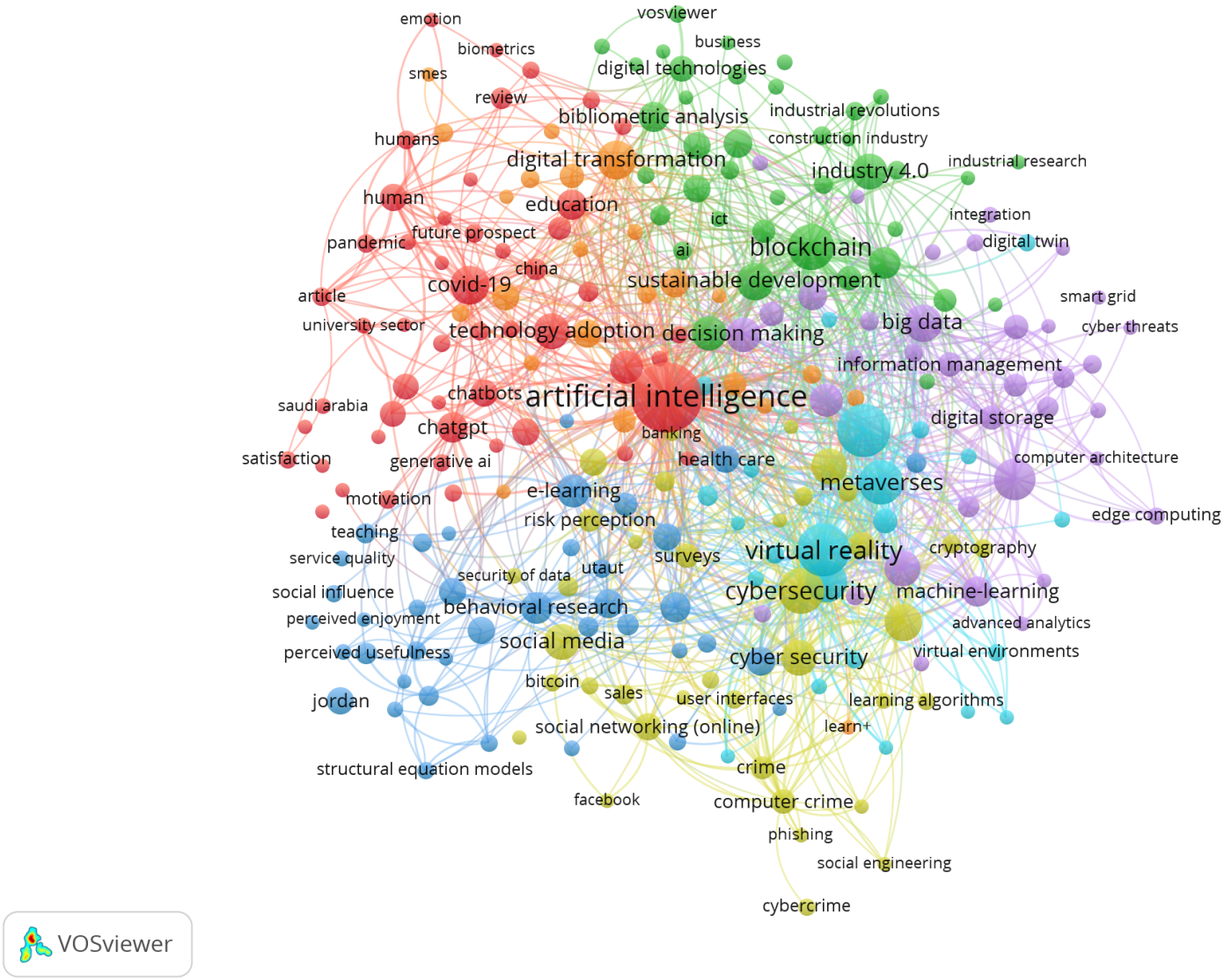

Figure 2. Keyword analysis.

co-occurrence network is visualized in Figure 2, which illustrates the clustering structure and thematic associations among the key terms.

A complex web of cybersecurity research patterns in virtual tourism becomes evident through the co-occurrence visual analysis of complete keyword variables. A compact visual network displays keyword nodes densely arranged around clusters and connects lines that emphasize the magnitude of relationship ties. Multiple color-coded thematic clusters illuminate major research areas including "data privacy" alongside "smart tourism" and "cybersecurity frameworks." Certain key research terms located in central positions act as instrumental elements connecting multiple research domains. The visualization succeeds in illustrating changing focus areas which provides enhanced knowledge about main research trends while revealing overlapping topics.

6.2 Co-Authorship Analysis of Countries

Co-authorship analysis examines the collaboration patterns between countries based on published research articles. It provides valuable insights into the international partnerships driving research in a specific domain, such as cybersecurity in virtual tourism. Table 2 presents the most productive authors in the field, ranked by their number of documents, citations, and total link strength in the collaboration network.

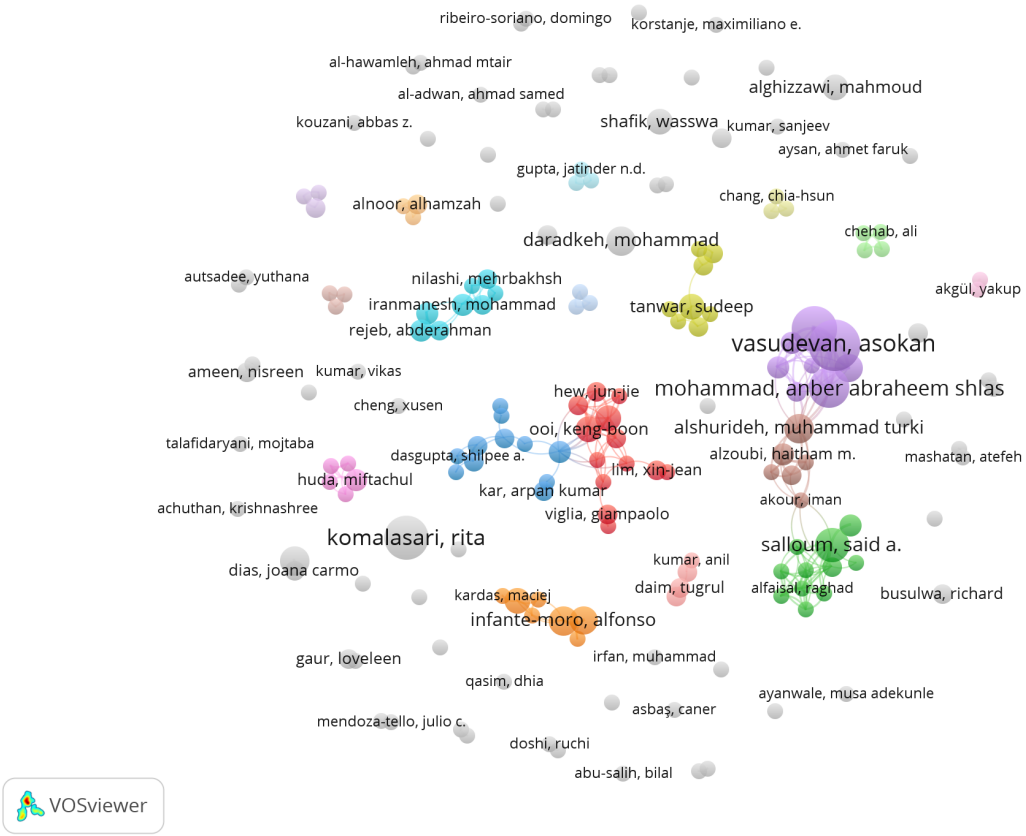

Figure 3. Co-authorship analysis of countries.

Table 1. Keyword contributions based on occurrences and total link strength.

Keyword	Occurrences	Total Link Strength
Artificial Intelligence	111	562
Metaverse	64	287
Virtual Reality	64	341
Cybersecurity	50	277
Blockchain	50	286
Metaverses	47	327
Internet of Things	41	240
Augmented Reality	40	216
Digital Transformation	36	129
COVID-19	36	149
Sustainable Development	32	160
Network Security	32	195
Big Data	32	200
Social Media	31	111
Industry 4.0	31	131
Technology Adoption	30	174
Cyber Security	30	192
Machine Learning	30	195
Security	29	162
Decision Making	28	172
Sustainability	27	120
Smart City	26	133

The main objective of studying co-authorship patterns between nations is to examine author cooperation patterns between different nations together with their research landscape implications. The analysis includes only authors who published at least two documents with at least one citation established. Among the total sample of 3350 authors only 175 authors qualify under the established research requirements according to the threshold settings.

Industrial analysis establishes co-authorship networks to study author collaboration through edge representations that show interactions between authors but nodes serve as individual authors. The computational strength of these edges depends on how many times authors published research together [18]. Scientists studying country-level collaboration patterns aggregate co-authorship data to determine the mechanisms through which countries engage with one another [19]. The database frequently supports evaluations regarding worldwide research patterns because it tracks citation results and border-spanning academic collaboration impacts [20]. The co-authorship network analysis demonstrates how international collaborations increase academic work visibility and citations

Table 2. Author contributions based on documents, citations, and total link strength.

Author	Documents	Citations	Total Link Strength
Mohammad, Sulieman Ibraheem	16	12	44
Mohammad, Anber Abraheem Shlash	13	12	44
Alshurideh, Muhammad Turki	7	62	26
Kuteishat, Ruba Jafar	6	12	23
Salloum, Said A.	9	359	22
Ooi, Keng-Boon	5	1017	21
Tan, Garry Wei-Han	5	1017	21
Alabda, Hamad Ejayan	4	12	18
Alkhamis, Faisal Abdulkarim	4	12	18
Al Oraini, Badrea	3	12	15
Al Mulhem, Ahmed	2	143	14
Alfaisal, Raghad	2	143	14
Alkhodour, Tayseer	2	143	14
Almaiah, Mohammed Amin	2	143	14
Awad, Ali Bani	2	143	14
Lutfi, Abdalwali	2	143	14
Dwivedi, Yogesh K.	4	329	13
Wong, Lai-Wan	3	822	13
Hew, Jun-Jie	3	694	12
Mohammad, Atallah Ibrahim	2	12	12
Infante-Moro, Alfonso	7	34	11
Alzoubi, Haitham M.	4	4	11

according to reports by both Liu et al. [32] as well as Hinrichs et al. [33] throughout their research. Studies by Barrett et al. [20] demonstrated citation rates increase after border-crossing collaborations according to their research. The global academic community demonstrates growing connection with a higher level of research collaboration leading to increased knowledge diffusion according to [30, 31]. Research by Wagner et al. [21] and Yu et al. [22] shows both knowledge dissemination effects and enhanced country research output from international research collaboration. The international collaboration network is visualized in Figure 3, which maps the co-authorship relationships among countries based on their joint publications in the field.

As shown in Figure 3, the network visualization reveals distinct clusters of collaborating countries, with the United States, United Kingdom, China, and Australia emerging as central hubs in the global research network. The thickness of connecting lines represents the intensity of collaboration between countries, illustrating strong research partnerships particularly among Western and Asian nations. This geographical analysis complements the author-level productivity data presented in Table 2, providing both micro and macro perspectives on research collaboration patterns in cybersecurity and virtual tourism.

6.3 Document Citation

A document citation examination serves to uncover the scholarly works which created the foundation for research in cybersecurity issues within virtual tourism. Virtual tourism integration with digital platforms has made protecting user data along with securing virtual environments an urgent requirement. Documents make up important landmarks which lead researchers in creating cybersecurity structures and solutions for this domain. The most influential publications in the field, as measured by their citation counts, are listed in Table 3.

A co-occurrence analysis of document citations about cybersecurity issues in virtual tourism used a citation threshold of minimum 7. The analysis covered 350 documents from a total of 1116 scholarly works because they reached at least seven times each in subsequent academic work. The chosen threshold serves as a defining criterion which enables the study to evaluate distinct academic contributions by determining which studies have made significant scholarly impact. This method emphasizes important academic publications as well as exposing new advances and prevalent concepts governing virtual

Table 3. Document citation analysis.

Document	Citations	Links
casino (2019)	1519	4
dwivedi (2022)	1242	1
dutta (2020)	893	1
buhalis (2019)	593	3
bodkhe (2020)	529	4
wong (2020)	499	0
krath (2021)	411	0
petropoulos (2022)	408	0
ometov (2021)	293	0
koo hang (2023)	270	4
loureiro (2021)	261	0
vlačić (2021)	253	0
jannach (2022)	237	0
abu-salih (2021)	235	0
ullah (2021)	220	0
ghobakhloo (2021)	206	0
kumar (2021)	198	0
yaacoub (2020)	194	0
gupta (2020)	190	1
chi (2020)	184	0
hassani (2020)	180	0
lee (2020)	180	0
wach (2023)	162	1

tourism and cybersecurity research. As illustrated in Figure 4, the citation network reveals how these key documents are interconnected through shared references and co-citation patterns.

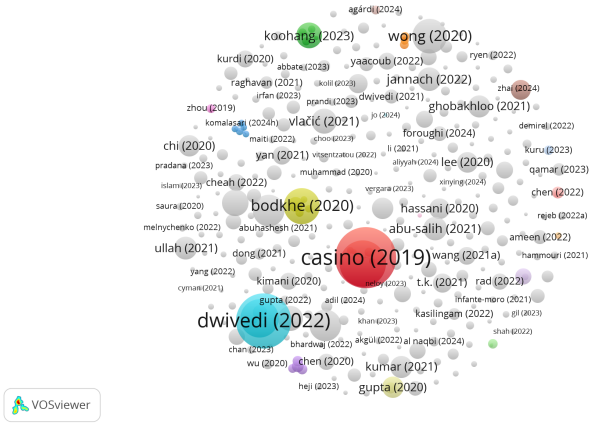

Figure 4. Overview of document citation analysis.

The visualization in Figure 4 shows the core-periphery structure of the citation network, with several seminal works (including those highlighted in Table 3) forming dense clusters of intellectual influence. Research articles with many citations help identify new cybersecurity methods which include encryption approaches together with authentication systems and AI-based detection frameworks created specifically for virtual tourism security. The research findings from these studies deliver technical intricacies alongside solutions for virtual environments' privacy challenges and user experiences. Highly cited papers have established benchmark approaches for secure virtual tourism systems which serve both academic discourse and real-world deployments.

6.4 Author Citaton

Through author citation analysis we understand the scientific influence researchers demonstrate in cybersecurity issues linked to virtual tourism. The frequency of academic peer citations enables us to evaluate both the academic standing and true importance of an author's work in this interdisciplinary field. Table 4 presents the most influential authors in cybersecurity and virtual tourism research, ranked by their citation impact and collaborative network strength.

Table 4. Author contributions based on documents, citations, and total link strength.

Author	Documents	Citations	Total Link Strength
Ooi, Keng-Boon	5	1017	7
Tan, Garry Wei-Han	5	1017	7
Buhalis, Dimitrios	2	863	9
Tanwar, Sudeep	5	829	10
Wong, Lai-Wan	3	822	7
Hew, Jun-Jie	3	694	0
Leong, Lai-Ying	2	679	0
Vigilia, Giampaolo	3	607	9
Kumar, Neeraj	3	548	6
Bodkhe, Umesh	2	533	7
Al-Turjman, Fadi	2	410	7
Salloum, Said A.	9	359	12
Iranmanesh, Mohammad	4	352	0
Dwivedi, Yogesh K.	4	332	7
Chehab, Ali	2	329	0
Noura, Hassan N.	2	315	0
Salman, Ola	2	315	0
Yaacoub, Jean-Paul A.	2	315	0
Cham, Tat-Huei	2	315	0
Ghobakhloo, Morteza	3	306	7
Koohang, Alex	2	270	0

An analysis of cybersecurity issues in virtual tourism shows that from a total of 3350 authors just 147 meet the criteria of writing two or more research papers with 44 or more citations. The established criteria reveal influential researchers and result in the selection of noteworthy academic contributors toward understanding field-shaping work.

Authors achieving these requirements receive recognition primarily because they continue to produce research and have made substantial contributions to cybersecurity discussions about virtual tourism. The purposes of requiring two published documents evaluate scholars' dedication to detailed research while citation numbers confirm the

academic importance of their work to researchers in their field.

This analytical table identifies prominent researchers along with influential scholars who showcase crucial collaboration patterns and their citations importance. The table shows how academic recognition requires high-impact research together with established academic networking. The citation network of these influential authors is visualized in Figure 5, which illustrates their interconnectedness and intellectual influence within the research domain.

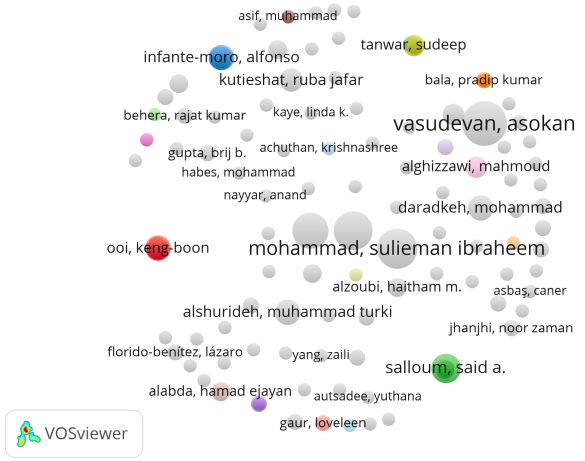

Figure 5. Most important authors based on author's citation network (processed using VOSViewer software).

As depicted in Figure 5, the network visualization clusters authors based on their citation relationships, revealing distinct research communities and highlighting key figures who serve as bridges between different thematic areas. The centrality and positioning of authors in this network, such as those listed in Table 4, reflect their role in shaping the intellectual structure of the field. Author citation analysis shows the way to map out field-based collaborative efforts and research inheritance relationships. Analysis of highly cited authors enables researchers to find leading experts who have established themselves as thought leaders in virtual tourism security discussions. Through this analysis researchers gain insights about scholars' individual achievements and witness how research themes evolve and knowledge spreads between related fields of study.

6.5 Co-Authorship Author Analysis

The analysis of co-authorship demonstrates how the research paper emerged from combined expertise which enabled study of cybersecurity challenges occurring during virtual decision processes. Different team members took charge of distinct responsibilities starting from data acquisition up through analysis and writing to create a streamlined production process. The most influential collaborative author networks are quantified in Table 5, which ranks authors by their combined productivity and citation impact within co-authored works.

Table 5. Author metrics.

Author	Documents	Citations	Total Link Strength
Casino, Fran	1	1519	2
Dasaklis, Thomas K.	1	1519	2
Patsakis, Constantinos	1	1519	2
Ooi, Keng-Boon	5	1017	37
Tan, Garry Wei-Han	5	1017	37
Butala, Richa	1	893	3
Choi, Tsan-Ming	1	893	3
Dutta, Pankaj	1	893	3
Somani, Surabhi	1	893	3
Buhalis, Dimitrios	2	863	25
Tanwar, Sudeep	5	829	24
Wong, Lai-Wan	3	822	28
Hew, Jun-Jie	3	694	13
Leong, Lai-Ying	2	679	8
Viglia, Giampaolo	3	607	9
Beldona, Srikanth	1	593	5
Bogicevic, Vanja	1	593	5
Harwood, Tracy	1	593	5
Hofacker, Charles	1	593	5
Kumar, Neeraj	3	548	17
Bodkhe, Umesh	2	533	7
Alazab, Mamoun	1	529	6

The unified approach to the research topic emerged because the authors from cybersecurity brought specialization with virtual decision-making insights through their backgrounds in related disciplines. A cohesive analytical pursuit took place throughout the study while ongoing communication and frequent exchanges of ideas produced alignment and research consistency. The joint authorship of the ultimate document leads to shared institutional and intellectual responsibility for resulted interpretations with distinct recognition of individual contributions. The structure and density of these collaborative relationships are visualized in the co-authorship network presented in Figure 6.

Figure 6 illustrates the filtering interface and resulting author network, revealing distinct collaborative clusters among the researchers listed in Table 5. The visualization demonstrates how authors with high total link strength, such as Ooi and Tan, serve as central hubs connecting multiple research groups. The image displays a user interface for filtering authors based on publication and citation thresholds, with two numerical input fields: The user interface includes two numeric fields for specifying document and citation

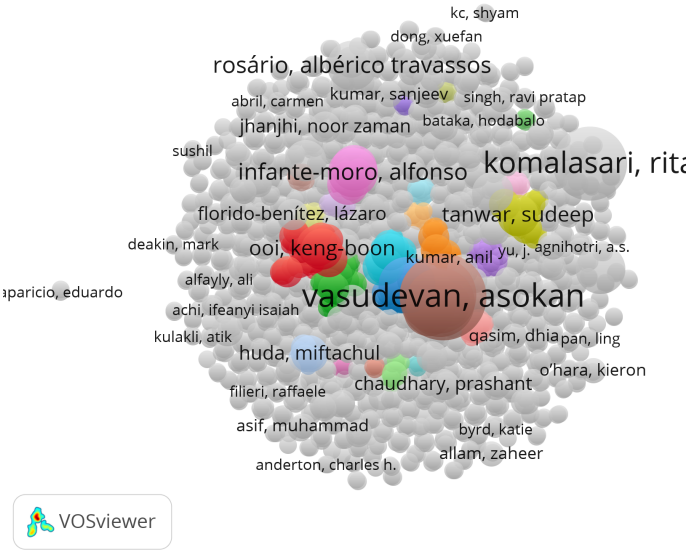

Figure 6. Co-authorship author analysis.

limits. Item 1 allows documents entered and a value of 1 is set while item 2 accepts citations with value 2. Both fields show a small question mark symbol for viewing supplemental details. A summary notes that 1,991 of the total 3,350 authors meet the defined requirements suggesting this information results from bibliometric analysis.

7 Conclusion

The scientometric analysis of cybersecurity research in virtual tourism presents a comprehensive understanding of the evolving landscape, shedding light on significant trends, influential authors, and prominent research connections. This study reveals that AI is the most frequently occurring keyword, appearing 111 times with 562 links. AI plays a major role in shaping research patterns, especially regarding automated systems and data protection strategies within virtual tourism. Closely associated with AI, the Metaverse shows a link strength of 287, while VR exhibits 341 connections, both highlighting their strong ties to virtual tourism principles. Furthermore, cybersecurity remains a cornerstone of virtual platform protection, occurring 50 times with a link strength of 277. These results bring out the intersection of AI, VR, and the Metaverse with cybersecurity, emphasizing both the emerging threats and opportunities for strengthening virtual tourism infrastructure [28, 29].

In spite of its notable citation count of 1519, Talukder et al. [23] maintains a link strength of 4, positioning it as a foundational work in virtual tourism cybersecurity. The high citation count paired with modest research connections suggests its role as a core reference point, while the research by Ghaderi et al. [24], with 1242 citations and a link strength of 1, highlights its recent yet impactful contribution to cybersecurity challenges in virtual tourism. Similarly, Dutta et al. [25] emerges with 893 citations and a link strength of 1, solidifying its relevance in specialized studies within the domain. These key works reveal the diverse components of cybersecurity discourse, establishing a strong academic foundation for protecting virtual tourism platforms.

Well-known scholars in the field include Ooi Keng-Boon and Tan Garry Wei-Han, who authored five papers that collectively gather 1017 citations and a link strength of 7. Their research gets significant recognition, casting moderate yet influential ties to core studies in cybersecurity. Dimitrios Buhalis, with only two published works, has acquired 863 citations and a link strength of 9, bringing out his extensive academic influence and his foundational role in virtual tourism studies [26]. Tanwar Sudeep leads with a link strength of 10; he has published five documents totaling 829 citations, further establishing himself as a critical figure in bridging cybersecurity and virtual tourism [27].

This scientometric breakdown highlights the vital need to address cybersecurity risks in virtual tourism by developing flexible security models, integrating AI-powered intrusion detection systems, and executing blockchain technology for secure transactions. The interlinking of AI, VR, and the Metaverse presents both challenges and opportunities, requiring continuous collaboration among scholars, policymakers, and technology developers. Taking care of global partnerships and standardizing cybersecurity frameworks, future research can build more resilient virtual tourism ecosystems, safeguarding user trust and ensuring sustainable growth. These findings serve as a cornerstone for advancing cybersecurity strategies, pushing the boundaries of innovation in virtual tourism platforms.

The future study should work towards the design of cross-border collaboration on security solutions between authorities based on extensive security protocols developed for measures of detection within virtual tourism platforms and the use of AI and blockchain technologies to mitigate future threats in cyberspace.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Balsalobre-Lorente, D., Driha, O. M., Shahbaz, M., & Sinha, A. (2020). The effects of tourism and globalization over environmental degradation in developed countries. *Environmental Science and Pollution Research, 27*(7), 7130-7144. [CrossRef]

[2] Kapoor, V. (2024). Artificial Intelligence and Cyber Security in the Service Industry. In *Artificial Intelligence for Smart Technology in the Hospitality and Tourism Industry* (pp. 265-303). Apple Academic Press.

[3] Becken, S., Whittlesea, E., Loehr, J., & Scott, D. (2020). Tourism and climate change: Evaluating the extent of policy integration. *Journal of sustainable tourism, 28*(10), 1603-1624. [CrossRef]

[4] Sharma, H., Srivastava, P. R., Jasimuddin, S. M., Zhang, Z. J., & Jebabli, I. (2024). Privacy concerns in tourism: a systematic literature review using machine learning approach and bibliometric analysis. *Tourism Review, 79*(5), 1105-1125. [CrossRef]

[5] Florido-Benítez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review. *Discover Computing, 28*(1), 28. [CrossRef]

[6] Masseno, M. D., & Santos, C. T. (2018). Assuring privacy and data protection within the framework of smart tourism destinations. *MediaLaws-Rivista di Diritto dei Media,*(2), 251-266.

[7] Pratisto, E. H., Thompson, N., & Potdar, V. (2022). Immersive technologies for tourism: a systematic review. *Information Technology & Tourism, 24*(2), 181-219. [CrossRef]

[8] Anwar, M. S., Ullah, I., Ahmad, S., Choi, A., Ahmad, S., Wang, J., & Aurangzeb, K. (2023). Immersive learning and AR/VR-based education: cybersecurity measures and risk management. In *Cybersecurity management in education technologies* (pp. 1-22). CRC Press.

[9] Ampountolas, A., & Li, J. (2025). Blockchain and the metaverse in tourism: A conceptual framework for decentralized OTAs. *Tourism Economics*, 13548166251399010. [CrossRef]

[10] Kovačić, M., Čičin-Šain, M., & Milojica, V. (2022). Cyber security and tourism: Bibliometric analysis. *Journal of process management and new technologies, 10*(3-4), 75-92. [CrossRef]

[11] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666. [CrossRef]

[12] Sinha, N., Dhingra, S., Sehrawat, R., Jain, V., & Himanshu. (2025). Customers' intention to use virtual reality in tourism: a comprehensive analysis of influencing factors. *Tourism Review, 80*(3), 742-766. [CrossRef]

[13] Calvaresi, D., Leis, M., Dubovitskaya, A., Schegg, R., & Schumacher, M. (2019). Trust in tourism via blockchain technology: results from a systematic review. *Information and communication technologies in tourism 2019, 304-317*. [CrossRef]

[14] Ramaseri-Chandra, A. N., & Pothana, P. (2024, October). Cybersecurity threats in Virtual Reality Environments: A Literature Review. In *2024 Cyber Awareness and Research Symposium (CARS)* (pp. 1-7). IEEE. [CrossRef]

[15] Alzahrani, N. M., & Alfouzan, F. A. (2022). Augmented reality (AR) and cyber-security for smart cities—A systematic literature review. *Sensors, 22*(7), 2792. [CrossRef]

[16] Ghaderi, Z., Beal, L., & Houanti, L. (2024). Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. *Current Issues in Tourism*, 1-16. [CrossRef]

[17] Loan, F. A., Bisma, B., & Nahida, N. (2022). Global research productivity in cybersecurity: a scientometric study. *Global Knowledge, Memory and Communication, 71*(4/5), 342-354. [CrossRef]

[18] Newman, M. E. (2001). The structure of scientific collaboration networks. *Proceedings of the national academy of sciences, 98*(2), 404-409. [CrossRef]

[19] Glänzel, W. (2014). Analysis of co-authorship patterns at the individual level. *Transinformação, 26*(3), 229-238. [CrossRef]

[20] Barrett, A. M., Crossley, M., & Dachi, H. A. (2011). International collaboration and research capacity building: Learning from the EdQual experience. *Comparative Education, 47*(1), 25-43. [CrossRef]

[21] Wagner, C. S. (2006). International collaboration in science and technology: Promises and pitfalls. *Science and technology policy for development, dialogues at the interface*, 165-176.

[22] Yu, H., Zhang, J., Zhang, M., & Fan, F. (2022). Cross-national knowledge transfer, absorptive capacity, and total factor productivity: The intermediary effect test of international technology spillover. *Technology Analysis & Strategic Management,*

34(6), 625-640. [CrossRef]

[23] Talukder, M. B., Kabir, F., Horaira, M. A., & Kumar, S. (2025). Challenges and Future Directions for the Use of AI and Security Intelligence in Tourism Industry. *The AI Metaverse Revolution: Transforming Multi-business Scenarios* (Volume 1), 165-178. [CrossRef]

[24] Ghaderi, Z., Beal, L., & Houanti, L. (2024). Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. *Current Issues in Tourism*, 1-16. [CrossRef]

[25] Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review, 142*, 102067. [CrossRef]

[26] Buhalis, D. (2020). Technology in tourism-from information communication technologies to eTourism and smart tourism towards ambient intelligence tourism: a perspective article. Tourism review, 75(1), 267-272. [CrossRef]

[27] Sharma, S., Gautam, A., & Tyagi, R. (2024, August). Artificial Intelligence and Cyber Security Driven Social Innovations in Digital Adventure Tourism. In *2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT)* (pp. 1-6). IEEE. [CrossRef]

[28] Bhattacharya, P., Saraswat, D., Dave, A., Acharya, M., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Coalition of 6G and blockchain in AR/VR space: Challenges and future directions. *IEEE Access, 9*, 168455-168484. [CrossRef]

[29] Xu, D., Pearce, P. L., & Chen, T. (2021). Deconstructing tourist scams: A social-practice-theory perspective. *Tourism Management, 82*, 104186. [CrossRef]

[30] Mêgnigbêto, E. (2015). Effect of international collaboration on knowledge flow within an innovation system: a Triple Helix approach. *Triple Helix, 2*(1), 1-21.

[31] Tan, C. N. L. (2016). Enhancing knowledge sharing and research collaboration among academics: the role of knowledge management. *Higher education, 71*(4), 525-556. [CrossRef]

[32] Liu, J., Chaminade, C., & Asheim, B. (2015). The geography and structure of global innovation networks: A knowledge base perspective. In *Global and Regional Dynamics in Knowledge Flows and Innovation* (pp. 140-157). Routledge.

[33] Hinrichs, M. M., Seager, T. P., Tracy, S. J., & Hannah, M. A. (2017). Innovation in the Knowledge Age: implications for collaborative science. Environment Systems and Decisions, 37(2), 144-155. [CrossRef]

Naveen Bhamasia received the M.Sc. degree in Mathematics from Central University of Himachal Pradesh, Dharamshala, India, respectively. He is currently pursuing a Ph.D. Degree from Central University of Himachal Pradesh, Dharamshala. His research interests include digital signature, authentication, and Blockchain technology. (Email: vlogs5575@gmail.com)

Garima Thakur received the M.Sc. degree from Central University of Himachal Pradesh, Dharamshala. She is currently pursuing the PhD Degree from Central University of Himachal Pradesh, Dharamshala. Her research interests include authentication, Post quantum cryptography, IoT and Blockchain technology. (Email: garima48451@gmail.com)

Sunil Prajapat received his M.Sc. degree in Mathematics from the Central University of Himachal Pradesh, Dharamshala, India. He recently completed his Ph.D. from the Srinivasa Ramanujan Department of Mathematics at the same university. He is currently serving as a Research Fellow at Gachon University, South Korea. His research interests, post-quantum cryptography, Post-Quantum Security, Mathematical Modelling, Machine Learning, Quantum Networks, Secure IoT. and the real- world implementation of cryptographic primitives. He has published extensively in reputed international journals and conferences and has contributed significantly to the fields of cryptographic security and quantum communication. Dr. Prajapat is is a recipient of the CSIR Junior Research Fellowship (JRF) and is a professional member of IEEE. He serves as a reviewer for IEEE, Elsevier, Springer, and MDPI journals and as Guest Editor for IEEE JBHI and IEEE Communications Standards Magazine. He has also served as an invited speaker, session chair, and track chair at various international conferences. (Email: sunilprajapat645@gmail.com)

Pankaj Kumar received the M.Sc. from CCS University Meerut India, M.E. from Thapar University and Ph.D. degrees from Galgotias University in 2005 and 2020, respectively. He has been an assistant professor at Srinivasa Ramanujan Department of Mathematics in the Central University of Himachal Pradesh, Dharamshala H.P. He has published more than 60 research papers in various SCI and SCIE-indexed journals and reputed conference, such as IEEE Communications Surveys and Tutorials, IEEE Transactions on Vehicular Technology, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Intelligent Transportation Systems, and IEEE Internet of Things Journal. His current research interests include quantum and post-quantum cryptography, information security as well as ML/AI. He is on the editorial board of many international journals of high repute, including IEEE, Wiley, and others, including SCI and SCIE journals, such as; International Journal of Communication Systems (Wiley), Security and Privacy Journal (Wiley). He has been involved in the research community as a technical program committee member or a PC chair for more than a dozen international conferences of high repute. He also serves as a reviewer for dozens of reputed journals, including SCI-Indexed Journals, published by IEEE, Elsevier, Springer, Wiley, and Taylor & Francis. (Email: pkumar240183@gmail.com)