Quest Journal of Management and Social Sciences
Volume 8 Issue 2: 509-521
ISSN Print: 2705-4527
ISSN Online: 2705-4535
Web: https://www.quest.edu.np

Users' Perceptions of Cybersecurity in the Banking Sector: A Bibliometric Study

Niruta Subedi[1], Ramesh Kunwar[1] & Majibur Rahman Siddique[2]*

[1]Quest International College, Pokhara University, Nepal
[2]Quest Research Management Cell, Quest International College, Pokhara University, Nepal
*Corresponding Author: ramesh@quest.edu.np

Received:15 March 2026
Revised: 23 April 2026
Accepted: 27April 2026
Published: 30 June 2026

How to cite this paper:
Subedi, N., Kunwar, R., & Siddique, M. R. (2026). Users' Perceptions of Cybersecurity in the Banking Sector: A Bibliometric Study. *Quest Journal of Management and Social Sciences, 8*(2), 509-521. https://doi.org/10.3126/qjmss.v8i2.96203

Abstract

Background: The rapid expansion of digital banking has intensified cybersecurity concerns for financial institutions and users. Despite increasing scholarly attention, research on users' perceptions of cybersecurity in the banking sector remains fragmented and lacks a clearly organized thematic structure.

Purpose: This study aims to map and synthesize the existing literature on user perceptions of cybersecurity in the banking sector by identifying major themes, research trends, collaboration patterns, and gaps in the field.

Design/methodology/approach: A bibliometric analysis was conducted using 669 articles retrieved from the Dimensions database. The dataset was analyzed using Biblioshiny (Bibliometrix package) and VOSviewer to examine publication trends, keyword structures, thematic development, source productivity, and international collaboration networks.

Findings: The results show that research on user perceptions of cybersecurity in banking has increased steadily since 2009, with the highest publication output occurring during 2023–2024. Keyword analysis indicates that cybersecurity (318 occurrences) is the dominant theme, followed by perceptions (70), cyber (58), and security (57), reflecting strong emphasis on user awareness, perceived risks, and digital safety. Lecture Notes in Computer Science emerged as the most productive publication outlet, followed by Computers & Security, SSRN Electronic Journal, and Information and Computer Security. The collaboration network identified the United States, the United Kingdom, and China as the leading contributors and collaboration hubs in the field.

Conclusion: Research on user perceptions of cybersecurity in the banking sector is growing steadily but remains concentrated around a limited number of dominant themes, sources, and contributing countries. The findings highlight increasing academic interest in cybersecurity risks, awareness, and user behavior in digital banking, while also indicating substantial opportunities for future research to deepen theoretical, empirical, and cross-country understanding of cybersecurity perceptions in financial services.

Keywords: Cybersecurity, user perception, digital banking, bibliometric analysis, information security

1. Introduction

The rapid digitization of financial services has fundamentally transformed how individuals interact with banking institutions, creating both opportunities for enhanced service delivery and unprecedented vulnerabilities to cyber threats. Cybersecurity, broadly defined as the protection of software, computers, and networks from malicious intrusion through tools encompassing authentication, encryption, and intrusion detection (Amoroso, 2006), has emerged as a critical concern within the financial sector. More comprehensively, it constitutes a collection of interconnected procedures designed to protect cyberspace-enabled systems from intentional acts that could result in a mismatch between a resource owner's perceived and actual property rights (Cavelty, 2014). As banking systems increasingly migrate to digital platforms, the intersection of cybersecurity and financial stability warrants urgent academic attention, particularly given that banking vulnerabilities have historically precipitated systemic financial crises. The growing frequency of cyberattacks targeting the financial sector underscores the nonlinear and complex nature of systemic banking risk, where a single breach can cascade into broader institutional instability.

In emerging economies, these challenges are acutely pronounced. Nepal presents a particularly instructive case: cybersecurity crimes have proliferated across multiple sectors, with financial institutions bearing a disproportionate burden. Estimated annual losses to Nepalese banks from cyber fraud amount to approximately NPR 50 million, encompassing both direct fraudulent transactions and indirect costs associated with incident response and system recovery (Subedi, 2015). The regulatory landscape remains underdeveloped; while Nepal Rastra Bank (NRB) serves as the primary oversight body, the absence of a robust cybersecurity law, skilled workforce, and proactive policy framework has constrained the country's capacity to mount effective defenses against evolving cyber threats. Compounding this challenge, survey data indicate that approximately 60% of banking customers express discomfort with online banking services due to perceived security risks, a finding with direct implications for digital adoption, customer retention, and the broader trajectory of Nepal's financial inclusion agenda.

Despite a substantial body of international research examining cybersecurity awareness, organizational preparedness, and technology adoption, scholarship focused specifically on banking customers' perceptions in the Nepalese context remains conspicuously sparse. Existing domestic studies have predominantly adopted organizational or technical perspectives, exploring institutional barriers and security challenges at the systemic level (Khatri & Mishra, 2024) or investigating the relationship between fintech growth and cybersecurity readiness among bank employees (Shrestha, 2023), without adequately capturing how ordinary users understand, trust, or engage with cybersecurity measures. This gap is significant, as global research has consistently identified fraud prevention efficacy (Nuseir et al., 2024), top management support (Alkhater, 2021), system complexity (Sharma & Wu, 2024), and security perceptions as determinants of mobile banking intentions (Uduimoh et al., 2019). Within Nepal's evolving digital banking landscape, users remain acutely vulnerable to threats such as phishing, SIM-swapping, and OTP fraud, and trust continues to erode in the wake of repeated cyber incidents, a dynamic that the Technology Acceptance Model (TAM) suggests can be partly mitigated if security features are perceived as both useful and usable, particularly among digitally literate younger populations.

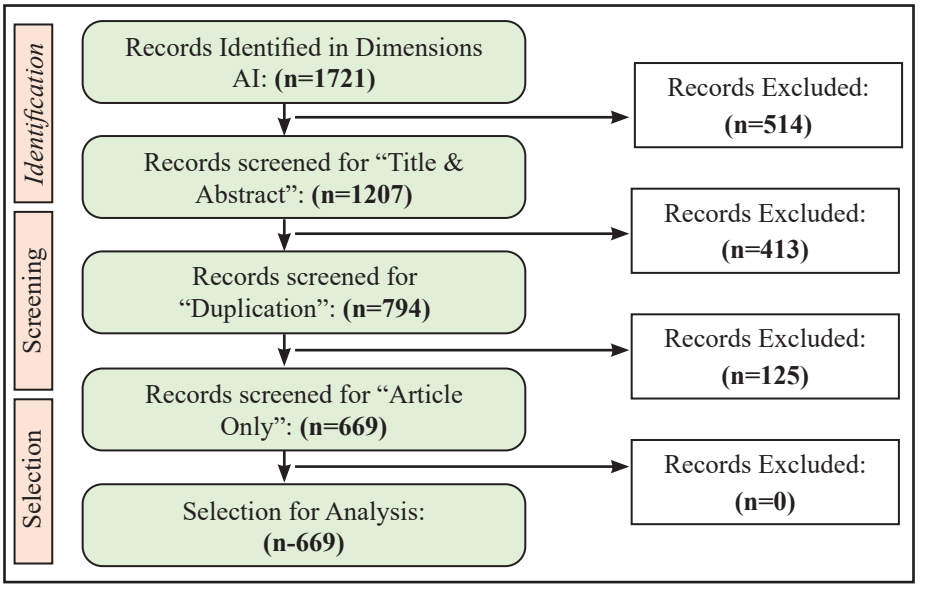
Against this backdrop, the present study employs a bibliometric methodology to systematically map the intellectual landscape of cybersecurity research within the banking sector, with particular attention to user perception as an underexplored dimension. Bibliometric analysis offers a rigorous, data-driven approach to identifying dominant themes, influential contributors, and structural gaps within a body of literature. This study pursues two primary objectives: (1) to methodically examine the current state of cybersecurity research as it pertains to banking users' perceptions, and (2) to identify key research gaps that can inform and direct future empirical and policy-oriented investigations, especially in underrepresented contexts such as Nepal. By doing so, this paper aims to contribute both to the global scholarly conversation on cybersecurity and to the evidence base needed to strengthen Nepal's digital banking security landscape.

2. Methodology

This study employed bibliometric analysis to systematically map and evaluate the scientific literature on users' perceptions of cybersecurity in the banking sector. Bibliometric analysis is a well-established quantitative approach that enables researchers to assess, visualize, and interpret research trends, intellectual structures, and knowledge evolution within a given field over time (Donthu et al., 2021). Data were sourced from Dimensions AI, a comprehensive academic database encompassing more than 159 million publications, selected for its extensive multidisciplinary coverage and suitability for large-scale bibliometric investigations (Siddique et al., 2026).

Figure 1

Data Selection Process



The document selection process followed three stages: identification, screening, and selection (see Figure 1). In the identification stage, a structured keyword search using the terms "cybersecurity" AND "perception" yielded an initial dataset of 1,721 publications. During the screening stage, titles and abstracts were reviewed, resulting in the exclusion of 514 records. An additional 413 duplicate records were removed, and 125 publications that were not journal articles were excluded. Consequently, a total of 1,052 records were eliminated during the screening phase. In the final selection stage, 669 journal articles met the inclusion criteria and were retained for analysis.

The retained dataset was analyzed using two complementary tools: the bibliometrix package in R and VOSviewer, each serving a distinct analytical function. Bibliometric analysis was conducted in two phases: performance analysis and science mapping following Siddique et al. (2026). Performance analysis, conducted via bibliometrix, assessed research productivity metrics including publication output, citation impact, and the identification of influential authors and journals (Basnet et al., 2024). Science mapping, facilitated by VOSviewer, was employed to explore thematic structures, conceptual clusters, and the intellectual evolution of cybersecurity perception research through co-citation analysis, keyword co-occurrence mapping, and bibliographic coupling (Lowar et al., 2025). Together, these methodological layers ensured that both the quantitative dimensions of research output and the qualitative contours of knowledge organization were systematically captured. This structured, transparent, and replicable procedure enhances the reliability of findings and provides a comprehensive foundation for identifying patterns, gaps, and future directions in the literature.

3. Results

Bibliometric analysis is a quantitative research method used to examine and evaluate large volumes of scientific literature by analyzing publication patterns, thematic developments, and research influence (Passas, 2024). In this study, two major bibliometric techniques, performance analysis and science mapping, were conducted using Biblioshiny, the web-based interface of the Bibliometrix R package. Performance analysis assesses research productivity and impact through indicators such as annual scientific output and source production over time (Belter, 2015). Science mapping, on the other hand, explores the conceptual and intellectual structure of the research field. It provides visual representations, including word clouds, thematic maps, and treemaps, which help identify key themes, emerging trends, and the evolution of research topics within the literature (Chen et al., 2023). Collectively, these techniques offer a comprehensive understanding of how research on users' perceptions of cybersecurity in the banking sector has developed, evolved, and interconnected over time.

3.1 Performance Analysis

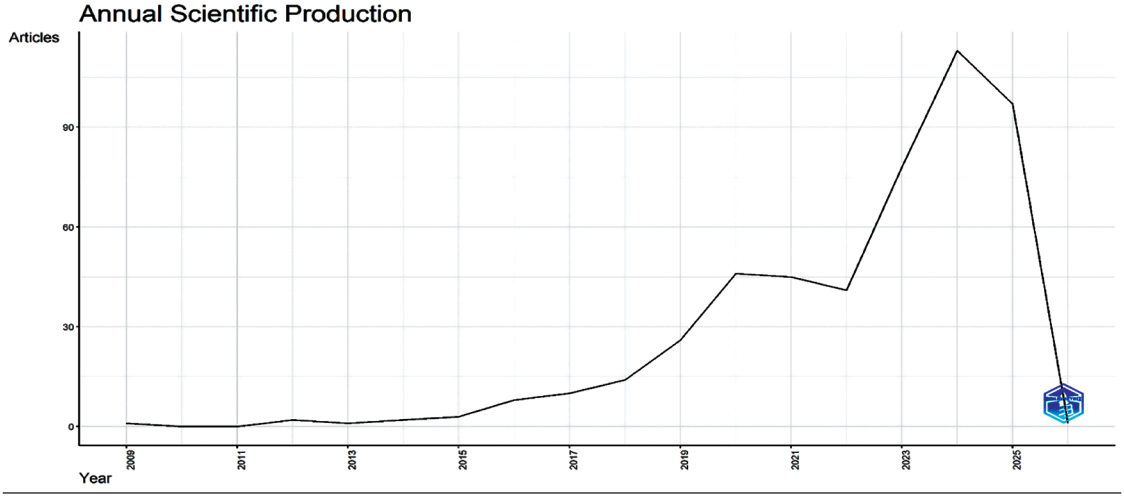
According to Siddique et al. (2026), performance analysis is a systematic approach for evaluating research contributions based on indicators such as publication output, citation impact, and patterns of scholarly collaboration. It aims to assess the growth and development of a research field while identifying the most influential authors, institutions, and sources contributing to its advancement. In this study, performance analysis is conducted using three key indicators: annual scientific production, sources over time, and average citations per year. These measures provide insights into the productivity, impact, and evolution of research on users' perceptions of cybersecurity in the banking sector.

3.1.1 Annual Scientific Production Analysis

Figure 2 illustrates the trend in annual scientific production related to users' perceptions of cybersecurity in the banking sector. The findings reveal that research activity in this area remained relatively limited until around 2015, after which publication output began to increase steadily, coinciding with the rapid expansion of digital banking services. Early scholarly contributions were sparse, with only 1 publication recorded in 2009, 2 in 2012, 3 in 2015, and 8 in 2016. Research activity started to gain momentum in 2017 with 10 publications and continued to grow in 2018 and 2019, reaching 15 and 26 publications, respectively. A more pronounced increase is evident from 2020 onward, with 48 publications in 2020 and 47 publications each in 2021 and 2022. The field experienced substantial growth in recent years, producing 80 publications in 2023 and reaching a peak of 117 publications in 2024. Although data for 2025 are not yet complete, the dataset already includes 98 publications, indicating sustained and growing scholarly interest in users' perceptions of cybersecurity within the banking industry.

Figure 2

Annual Scientific Production

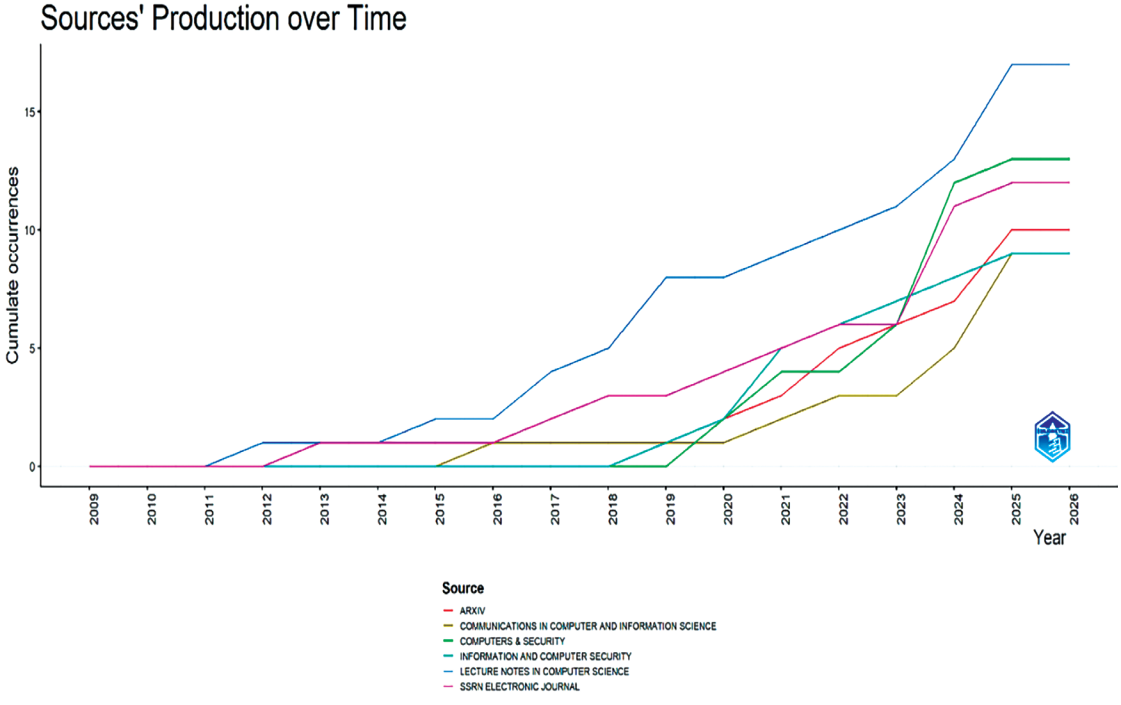


3.1.2 Sources Production Overtime Analysis

Figure 3 presents the source production over time for the five most productive publication sources in the field. The results indicate a steady increase in contributions across these sources, reflecting the growing academic interest in cybersecurity research. Lecture Notes in Computer Science demonstrated a consistent upward trend, reaching 4 publications in 2025. Similarly, arXiv showed notable growth, increasing from a single publication in 2019 to 4 publications in 2025. SSRN Electronic Journal maintained relatively low publication levels in earlier years but experienced a sharp increase in 2024, recording 5 publications and highlighting its growing importance as a research outlet. Computers & Security began contributing to the datast in 2020 and reached its highest publication output in 2024, underscoring its prominent role in cybersecurity scholarship. Meanwhile, Information and Computer Security exhibited a stable publication pattern, contributing between 1 and 3 articles annually. Overall, the publication trends across these leading sources reveal a significant rise in research activity since 2020, corresponding with the increasing global focus on cybersecurity challenges and user-related security concerns.

Figure 3

Sources Production Overtime

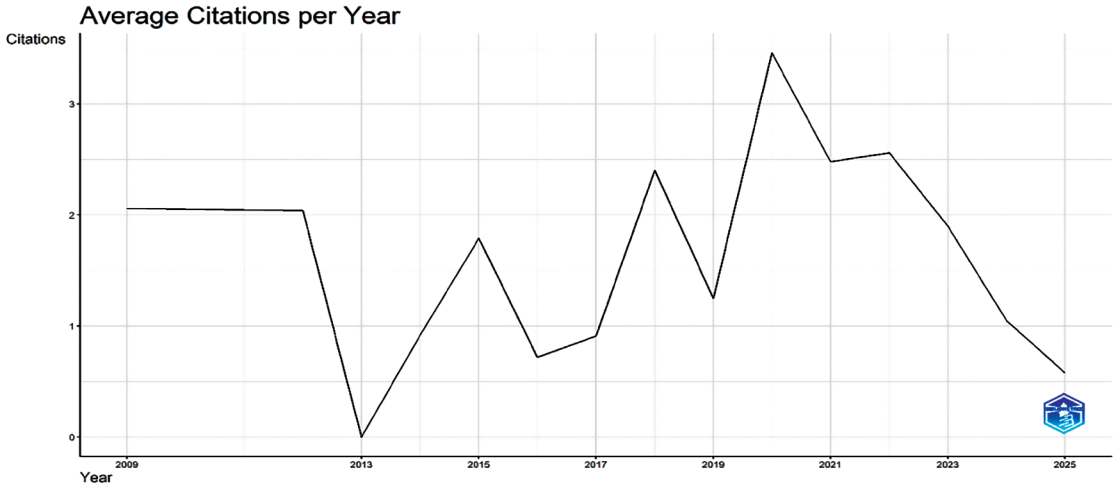


3.1.3 Average Citations Per Year Analysis

Figure 4 illustrates the trend in average citations per year, revealing notable variations over time. During the early years, the average citation rate remained relatively stable at approximately two citations per publication. However, a sharp decline was observed in 2012 and 2013, when the average citation count dropped to nearly zero. Following this period, citation impact gradually increased, reaching its highest level in 2020 with an average of approximately 3.5 citations per publication, indicating strong scholarly recognition and influence. Since 2021, however, the trend has shown a consistent decline, with average citations falling to fewer than one citation per publication in recent years. This decrease is likely attributable to the recency of these publications, as newly published studies generally require time to accumulate citations. Consequently, while research output in the field has continued to expand, the citation impact of recent publications has not yet fully materialized.

Figure 4

Average Citation Per Year

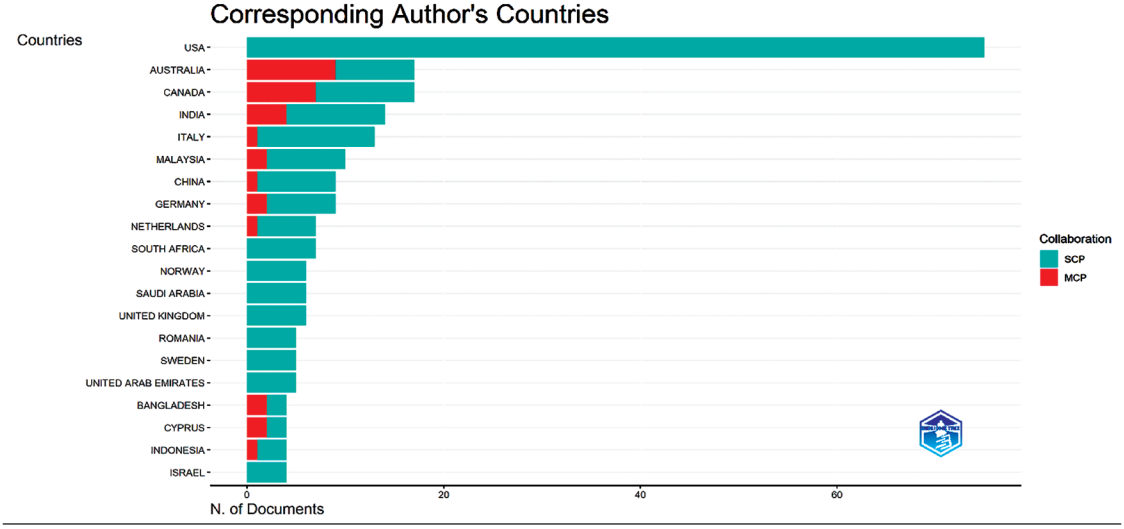


3.1.4 Corresponding Authors' Countries Analysis

Figure 5 presents the distribution of authors' countries, highlighting the research contributions and collaboration patterns across nations. The United States emerges as the leading contributor, with the majority of its publications originating from single-country publications (SCP), indicating strong domestic research activity. Australia and Canada also demonstrate substantial research output, supported by both single-country publications and multi-country publications (MCP), reflecting a balance between national productivity and international collaboration. Other countries, including India, Italy, Malaysia, China, and Germany, exhibit moderate levels of research output, suggesting their increasing engagement in studies related to cybersecurity perceptions. In contrast, countries such as Bangladesh, Cyprus, Indonesia, and Israel contribute a smaller number of publications and display relatively limited international collaboration. Overall, the figure indicates that while research productivity is concentrated in a few leading countries, collaborative research efforts are becoming increasingly common across various regions, fostering the global development of knowledge in the field.

Figure 5

Corresponding authors' countries

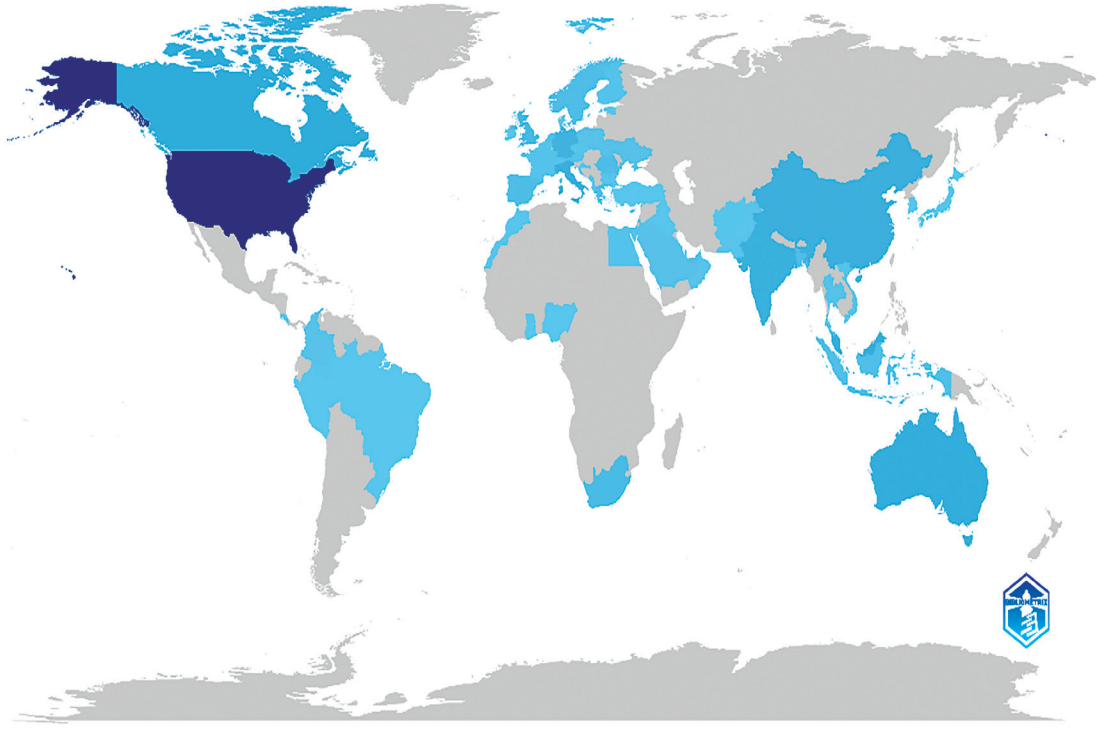


3.1.5 Countries Scientific Production Analysis

Figure 6 illustrates the global distribution of scientific production related to users' perceptions of cybersecurity in the banking sector. The map indicates that research activity is predominantly concentrated in developed countries. The United States emerges as the leading contributor, represented by the darkest shade on the map, reflecting the highest level of scientific output. Other major contributors include Australia, Canada, the United Kingdom, Germany, China, and India, which are also depicted in darker shades, signifying substantial research productivity. Several countries across Europe, Asia, and Africa demonstrate moderate levels of contribution, while many nations in South America, Africa, and the Middle East exhibit limited or no research output in this area. Overall, the map highlights the global nature of research on cybersecurity perceptions while revealing that a relatively small group of highly productive countries continues to dominate scholarly contributions in the field.

Figure 6

Countries scientific production

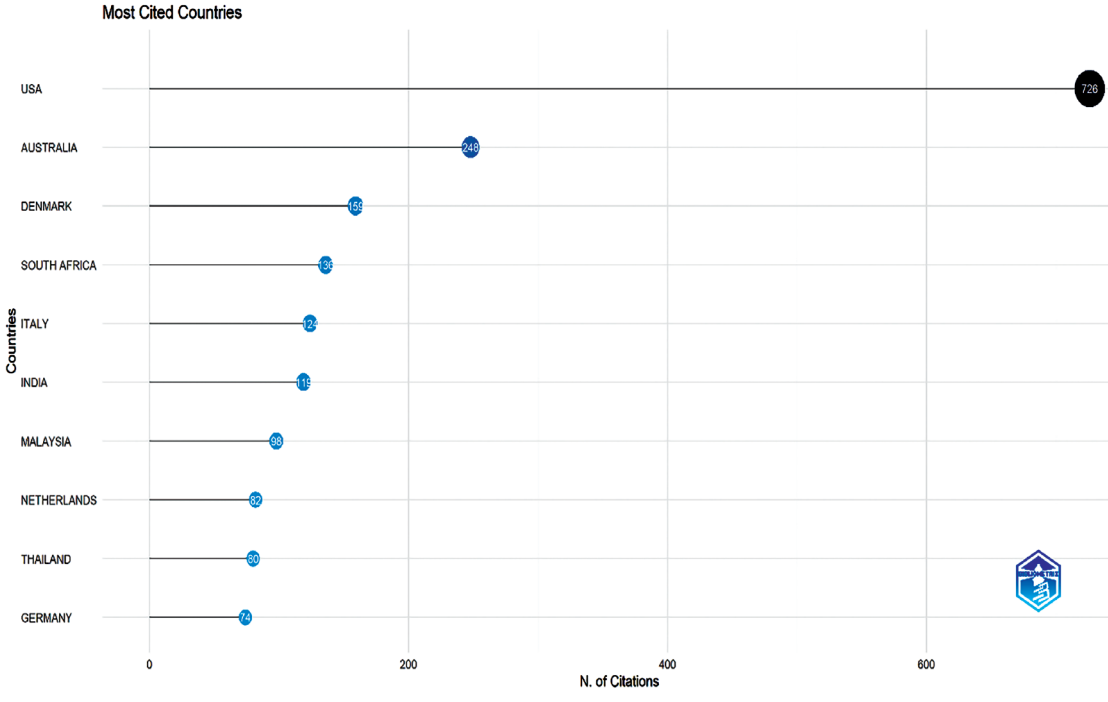


3.1.6 Most Cited Country Analysis

Figure 7 presents the distribution of citations by country, highlighting the global impact and influence of research in the field. The United States ranks first with 728 citations, making it the most influential contributor to the literature. Australia follows with 248 citations, while Denmark and South Africa have also achieved significant research impact, recording 135 and 128 citations, respectively. Countries such as Italy (72 citations), India (71 citations), and Malaysia (50 citations) demonstrate moderate citation performance, reflecting their growing involvement and influence in the research area. Meanwhile, the Netherlands (32 citations), Thailand (30 citations), and Germany (27 citations) have comparatively lower citation counts but continue to contribute valuable scholarly work. Overall, the citation distribution indicates that research influence is concentrated in a few leading countries, while a broader group of nations contributes steadily to the advancement of knowledge within the field.

Figure 7

Most cited countries



3.2 Science Mapping

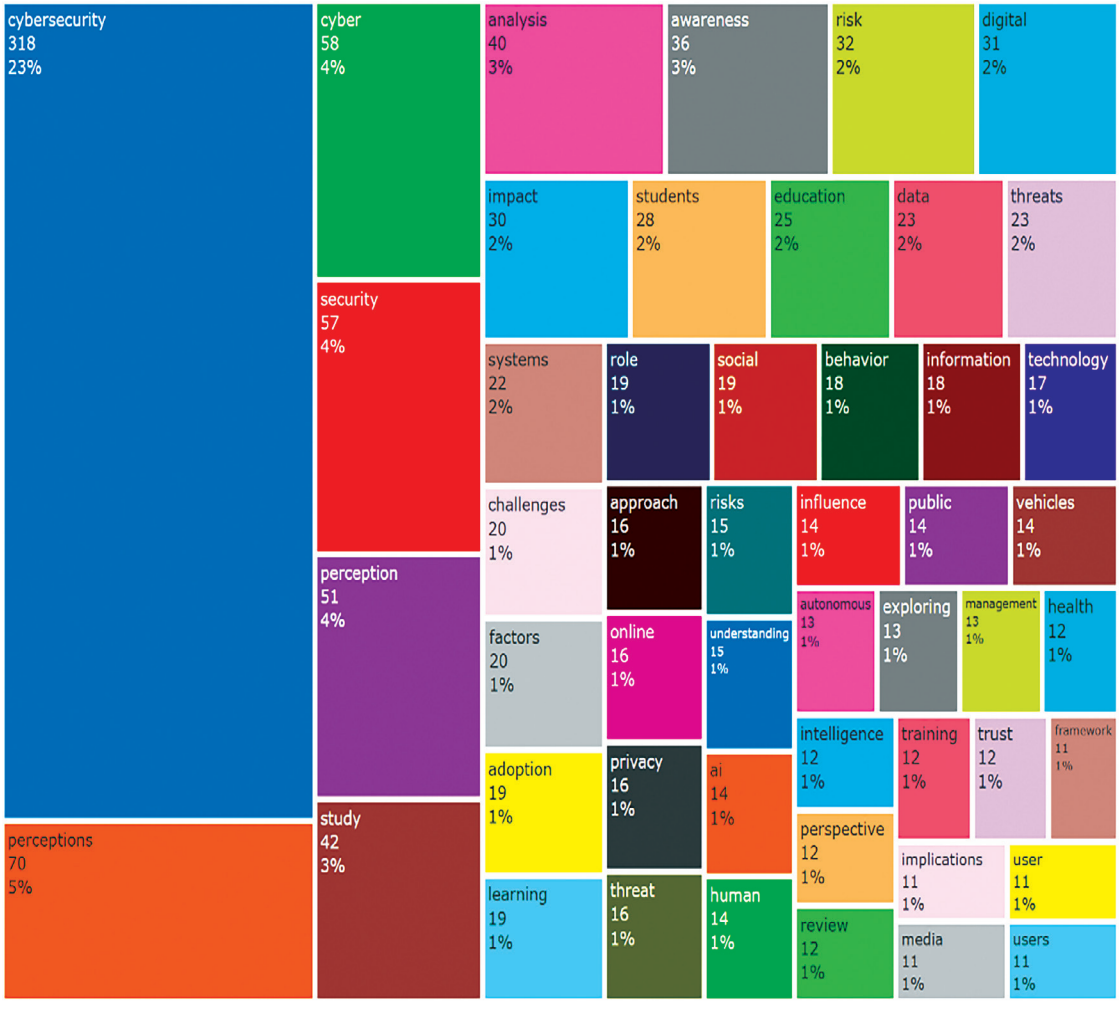
Science mapping is a bibliometric technique used to visualize and analyze the intellectual structure, relationships, and evolution of knowledge within a research field over time (Chen, 2017; Siddique et al., 2026). It identifies key themes, research clusters, and connections among keywords, authors, and topics, thereby providing insights into well-established, emerging, and declining areas of study (Lowar et al., 2025). In this research, science mapping is employed to examine the development of studies on users' perceptions of cybersecurity in the banking sector. The analysis highlights the major research themes, thematic clusters, and intellectual linkages that have shaped the field, offering a comprehensive understanding of its evolution and knowledge structure.

3.2.1 Tree Map Analysis

Figure 8 presents a treemap of the most frequently occurring keywords in the selected literature, illustrating the relative prominence of research themes within the field. The keyword "cybersecurity" dominates the treemap with 318 occurrences (23%), highlighting its central role in the literature. Other highly frequent keywords include "perceptions" (70 occurrences), "cyber" (58), "security" (57), and "perception" (51), indicating a strong emphasis on users' perceptions and cybersecurity-related issues. Keywords with moderate frequencies, such as "analysis" (40), "awareness" (36), "risk" (32), "digital" (31), "impact" (30), "students" (28), and "education" (25), suggest that a substantial body of research has focused on cybersecurity awareness, risk assessment, educational initiatives, and the broader impacts of cybersecurity challenges. Smaller keyword clusters, including "systems," "behavior," "technology," "privacy," "trust," "training," "AI," "public," and "management," represent emerging or specialized research areas that connect cybersecurity with human behavior, technology adoption, organizational management, and privacy concerns. Overall, the treemap demonstrates that while cybersecurity and user perceptions remain the dominant themes, research interest is increasingly expanding toward related topics such as awareness, risk, digital behavior, privacy, and technological innovation.

Figure 8

Tree Map

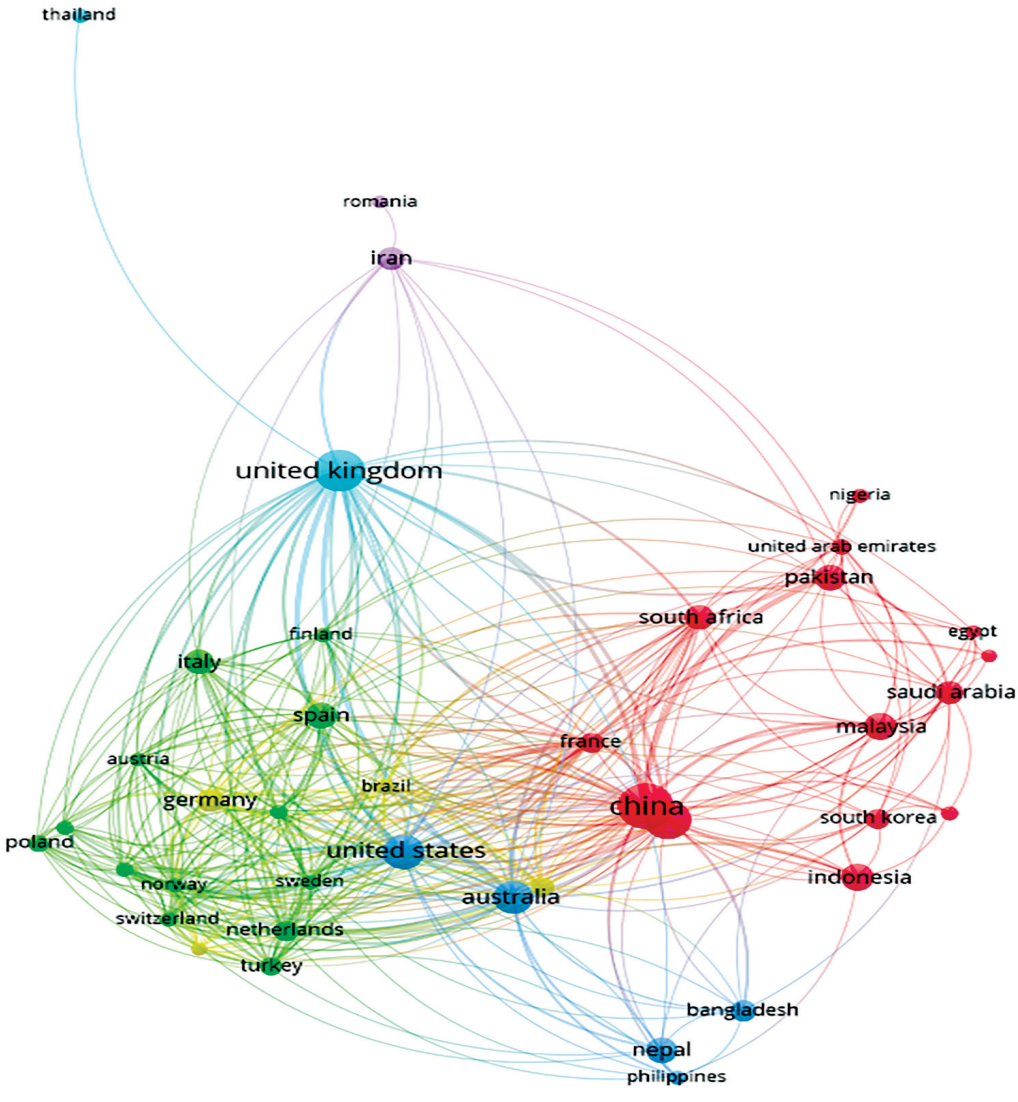


3.2.2 Country Collaboration Network

Figure 9 presents a VOSviewer network map illustrating international research collaboration in studies related to cybersecurity and users' perceptions within the banking sector. In the network, each node represents a country, with larger nodes indicating greater research productivity, while the connecting lines depict co-authorship and collaborative relationships among countries. The map identifies China, the United Kingdom, and the United States as the principal collaboration hubs, reflecting their significant research output and extensive international partnerships. China demonstrates strong collaborative links with countries such as Malaysia, South Africa, Saudi Arabia, and Indonesia. Similarly, the United Kingdom and the United States maintain broad research networks spanning multiple countries across Europe, Asia, and other regions. Smaller nodes, including Nepal, Thailand, and Romania, indicate relatively lower research output but highlight their emerging participation in international scholarly collaboration. Overall, the network reveals a highly interconnected global research landscape in which a few leading countries play a central role in shaping and advancing research on cybersecurity and user perceptions in the banking sector.

Figure 9

Country Collaboration Network

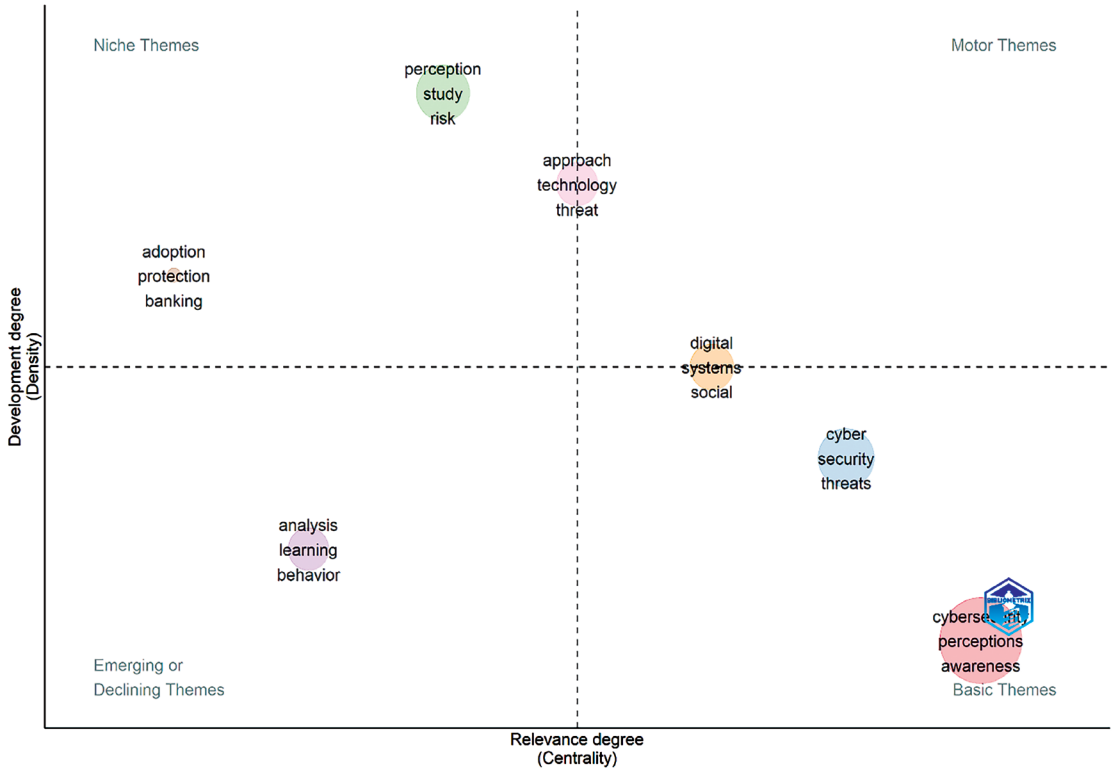


3.2.3 Thematic Map Analysis

Figure 10 presents the thematic map of research on users' perceptions of cybersecurity in the banking sector, classifying themes according to their degree of development (density) and relevance (centrality). The map is divided into four quadrants: Motor Themes, Niche Themes, Emerging/Declining Themes, and Basic Themes. The Motor Themes quadrant includes digital systems and social systems, indicating that these topics are both highly developed and highly relevant to the field. Niche Themes, represented by clusters such as perception, study, and risk, are well developed but less central, suggesting that they address specialized areas within the broader research domain. The Emerging/Declining Themes quadrant contains topics such as analysis, learning, and behavior, which exhibit low levels of development and centrality. These themes may either represent newly developing research directions or areas that are gradually losing scholarly attention.

Figure 10

Thematic Map



The Basic Themes quadrant is characterized by cybersecurity, perceptions, and awareness, which are highly relevant to the field but remain comparatively underdeveloped. As these themes form the foundation of research on cybersecurity and user perceptions in the banking sector, their placement indicates substantial opportunities for future investigation. The findings suggest that key topics such as cybersecurity awareness, risk perceptions, technological threats, trust, and digital banking adoption require further scholarly attention. Consequently, the thematic map highlights that the field is still evolving and offers considerable potential for future research aimed at understanding how users perceive cyber risks, develop security awareness, and make decisions regarding the adoption of digital banking services.

4. Discussion

The bibliometric analysis of cybersecurity, user perception, and digital banking demonstrates a substantial expansion of research activity over recent years, largely driven by the rapid digitalization of financial services and the increasing prevalence of cyber threats (Asmar & Tuqan, 2024). The annual publication trend reveals steady growth, particularly after 2019, reflecting heightened scholarly interest in understanding cybersecurity challenges and user behavior within digital banking environments. Country-level performance analysis indicates that the United States, Australia, Canada, India, Italy, and China are among the most productive contributors to the field. In terms of research impact, however, the United States, Australia, Denmark, and South Africa lead in citation performance, suggesting a stronger influence on the development of knowledge. Although countries such as Bangladesh, Malaysia, Thailand, and Germany have contributed to the literature, their relatively lower citation counts indicate that their influence remains comparatively limited and that their engagement in the field is still emerging (Lavanya & Rajkumar, 2024).

The science mapping results further highlight the intellectual structure of the field. The keyword treemap identifies cybersecurity, perception, security, awareness, risk, and digital as the most prominent themes, emphasizing the central role of user perceptions, threat awareness, and behavioral responses in digital banking contexts (Bukovec & Antoliš, 2024). Similarly, the international collaboration network reveals an uneven distribution of research partnerships. China, the United Kingdom, and the United States serve as major collaboration hubs, maintaining extensive co-authorship networks across regions. In contrast, countries such as Nepal, Thailand, and the Philippines occupy more peripheral positions, reflecting lower levels of international collaboration and research integration. These findings suggest that while cybersecurity in digital banking is a globally relevant topic, research capacity, knowledge production, and collaborative networks remain concentrated within a limited number of leading countries.

The thematic map provides additional insights into the maturity and future direction of the research domain. Cybersecurity, user perceptions, awareness, and threats are positioned within the Basic Themes quadrant, indicating that these topics are highly relevant but remain insufficiently developed and therefore require further investigation. In contrast, digital systems and social systems emerge as Motor Themes, reflecting their strong development and central importance within the broader research landscape (Cele & Kwenda, 2024). Niche Themes, including perception studies, risk, and technology-related approaches, represent specialized yet less influential areas of inquiry (Basnet et al., 2025). Meanwhile, analysis, behavior, and learning are categorized as Emerging or Declining Themes, suggesting either the early stages of development or a gradual decline in scholarly attention. Collectively, these findings indicate that cybersecurity and user perception in digital banking constitute a rapidly growing but still evolving field of study. Despite increasing research output, significant gaps remain in terms of thematic development, global participation, collaboration networks, and empirical understanding, highlighting the need for continued research and theoretical advancement in this important area.

5. Conclusion

This study examined the research landscape on cybersecurity and user perceptions in digital banking through a bibliometric analysis and highlighted the growing scholarly interest in the field. The findings indicate that although digital banking adoption is expanding rapidly in Nepal, users continue to face significant cybersecurity risks that influence their trust, perceptions, and adoption behavior. Issues such as limited cybersecurity awareness, low digital literacy, and increasing cyber fraud incidents reveal a gap between technological advancement and user preparedness. By identifying major research themes, influential countries, collaboration patterns, and emerging areas of inquiry, this study contributes to the existing literature by providing a comprehensive overview of the field and highlighting the need for stronger cybersecurity frameworks, user education initiatives, and institutional readiness within Nepal's banking sector. The findings offer valuable insights for policymakers, banking institutions, and researchers seeking to enhance cybersecurity resilience and promote secure digital banking adoption.

Despite its contributions, this study has several limitations. The analysis was based solely on the Dimensions database, which may not capture all relevant publications indexed in other databases such as Scopus or Web of Science. In addition, the study relied on bibliometric indicators and keyword-based analyses, which may not fully reflect the depth and contextual nuances of individual studies. Future research should incorporate multiple databases, larger datasets, and empirical investigations involving diverse user groups. Further studies may also explore the role of artificial intelligence-driven security tools, psychological and technological determinants of cybersecurity perceptions, real-world cyber incident data from banks, and cross-country comparative analyses to advance understanding of secure digital banking adoption and cybersecurity management.

References

Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*, e37571. https://doi.org/10.1016/j.heliyon.2024.e37571

Basnet, P., Devkota, N., Chapagain, R. K., & Mahapatra, S. K. (2024). Paving the way to the gig economy: A bibliometric analysis of workers' decade-long involvement. *Economic Journal of Nepal, 47*(1–2), 43–64. https://doi.org/10.3126/ejon.v47i1-2.80899

Basnet, R., Shakya, S., & Gautam, D. (2024). Science mapping and performance analysis in emerging research domains. *Journal of Informetrics, 18*(2), 1–15.

Belter, C. W. (2015). Bibliometric indicators: Opportunities and limits. *Journal of the Medical Library Association, 103*(4), 219–221. https://doi.org/10.3163/1536-5050.103.4.014

Chen, C. (2017). Science mapping: A systematic review of the literature. *Journal of Data and Information Science, 2*(2), 1–40. https://doi.org/10.1515/jdis-2017-0006

Chen, H., Tsang, Y., & Wu, C. (2023). When text mining meets science mapping in bibliometric analysis: A review and future opportunities. *International Journal of Engineering Business Management, 15*. https://doi.org/10.1177/18479790231222349

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13–21.

Dongol, R., & Chatterjee, J. M. (2019). Robust security framework for mitigating cyber threats in banking payment systems: A study of Nepal. *LBEF Research Journal of Science, Technology and Management, 1*(1), 61–81.

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. https://doi.org/10.1016/j.jbusres.2021.04.070

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing biometric systems for enhancing cybersecurity in the banking sector: A systematic analysis. *IEEE Access, 11*, 80181–80198. https://doi.org/10.1109/ACCESS.2023.3300668

Kumar, R. (2025). Bibliometric analysis: Comprehensive insights into tools, techniques, applications, and solutions for research excellence. *Spectrum of Engineering and Management Sciences, 3*(1), 45–62.

Lavanya, B., & Rajkumar, A. (2024). Bibliometric insights on mapping the landscape of cybersecurity: Uncovering the research potential in the banking industry. *Multidisciplinary Reviews, 7*(4). https://doi.org/10.31893/multirev.2024113

Lowar, D. B., Devkota, N., & Siddique, M. R. (2025). Mapping the global research on environmental, social, and governance (ESG): A bibliometric analysis. *NCC Journal, 10*(1), 69–88. https://doi.org/10.3126/nccj.v10i1.95031

Maharjan, R., & Chatterjee, J. M. (2019). Framework for minimizing cybersecurity issues in the banking sector of Nepal. *LBEF Research Journal of Science, Technology and Management, 1*(1), 82–98.

Mahato, S., Nayak, R. K., Raut, A. D., & Yadav, J. (2024). Electronic fraud (cyber fraud) risk in the banking industry of Nepal. *International Journal of Scientific Research in Engineering and Management, 8*, 1–12.

Maliha, H. (2025). Cybersecurity and fintech studies in academic discussion. *Journal of Islamic Economics Literatures*. https://doi.org/10.58968/jiel.v5i2.578

Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia, 4*(2), 1083–1097. https://doi.org/10.3390/encyclopedia4020065

Siddique, M. R., Devkota, N., Lowar, D. B., Paudel, U. R., Kunwar, R., & Lawaju, P. (2026). Responsible generative artificial intelligence for sustainable pedagogy systems: A conceptual framework for the Global South. *International Journal of Emerging Technologies in Learning, 21*(2), 4–29. https://doi.org/10.3991/ijet.v21i02.60809