Journal of Management Prospective (JMP)
Vol. 1, No. 1, June 2026
Received: 5 January 2026 | **Revised**: 18 February 2026 | **Accepted**: 24 March 2026

A Bibliometric Analysis of Cybersecurity Challenges Faced by Fintech Firms

Rakshya Bhandari

Nepal Commerce Campus, Tribhuvan University, Nepal

Abstract

Purpose: This study conducts a bibliometric analysis of cybersecurity challenges in the FinTech sector, focusing on emerging threats and vulnerabilities associated with digital financial technologies.

Methodology/Design/Approach: The study utilizes bibliometric analysis based on 311 articles retrieved from the Dimensions.ai database covering the period from 2016 to 2025. VOSviewer software was employed to analyze publication trends, co-citation patterns, and author collaboration networks.

Findings: The findings reveal a substantial growth in cybersecurity-related FinTech research, particularly after 2020, indicating increasing global concern regarding digital financial security. The study identifies leading contributors, influential publications, and collaborative research patterns within the field. It further highlights major cybersecurity challenges, including data breaches, privacy risks, and regulatory compliance issues arising from technologies such as artificial intelligence and blockchain.

Implications: The study emphasizes the importance of developing robust cybersecurity frameworks, regulatory mechanisms, and innovative technological solutions to strengthen secure digital financial ecosystems.

Originality/Value: This research provides a comprehensive bibliometric overview of cybersecurity issues in FinTech and offers valuable insights into emerging research directions and collaborative developments in the field.

Keywords: Cybersecurity, digital banking, data breaches, financial technology, fintech, payment systems

JEL Classification: D83, G23, L86, O33

---

*Correspondence: rakshyaab@gmail.com

Introduction

The rapid growth of financial technology (FinTech) has revolutionized the global financial services industry, providing enhanced accessibility, efficiency, and innovation in financial transactions. FinTech firms leverage digital platforms, artificial intelligence (AI), blockchain, cloud computing, and big data analytics to offer services such as mobile banking, digital payments, peer-to-peer lending, and robo-advisory solutions (Arner et al., 2016). However, this rapid digital transformation has also increased cybersecurity vulnerabilities, exposing the sector to risks such as data breaches, fraud, identity theft, and regulatory non-compliance (Zetzsche et al., 2018). With FinTech solutions relying heavily on interconnected digital infrastructures, ensuring robust cybersecurity frameworks has become a critical priority for financial institutions and regulatory bodies worldwide. Cybersecurity threats within FinTech are multifaceted, ranging from phishing attacks and ransomware to insider threats and API security breaches (Mishra & Kaushik, 2023). The integration of emerging technologies such as blockchain, cloud computing, and open banking APIs has introduced both new security solutions and vulnerabilities. For instance, while blockchain provides enhanced security through decentralized ledgers, it is not immune to smart contract vulnerabilities and cryptographic attacks (Karim et al., 2022). Similarly, open banking—driven by regulatory frameworks such as PSD2 (Revised Payment Services Directive)—has increased transparency but also heightened risks related to third-party access and API exploitation (Gupta et al., 2018). As FinTech adoption continues to expand, particularly in emerging economies, the need for comprehensive cybersecurity measures, compliance frameworks, and risk mitigation strategies becomes even more pressing.

Despite advancements in cybersecurity technologies, FinTech firms face persistent challenges, including regulatory uncertainty, lack of standardization, and evolving cyber threats (Deng, Qing, 2020). The financial sector remains a prime target for cybercriminals due to the high value of financial data and digital assets. Recent high-profile incidents, such as the SolarWinds cyberattack (2020) and the Capital One data breach (2019), highlight the vulnerabilities within financial digital infrastructures. Additionally, the rise of ransomware-as-a-service (RaaS) and AI-driven cyberattacks has further complicated the cybersecurity landscape, making proactive defense mechanisms essential (Miah et al., 2023). Given the increasing reliance on digital finance, there is an urgent need for research that systematically examines the evolving cybersecurity challenges faced by FinTech firms globally. This study aims to fill that gap by conducting a bibliometric analysis of existing research on cybersecurity threats in the FinTech sector. By leveraging data from Dimensions.ai and analyzing it using VOSviewer software, this research seeks to identify publication trends, co-citations, bibliographic coupling, co-authorship networks, and keyword co-occurrences related to cybersecurity in FinTech. The study not only tracks the global progress in understanding cybersecurity risks in FinTech but also explores the specific challenges faced by emerging markets, such as limited cybersecurity infrastructure, regulatory fragmentation, and insufficient awareness among stakeholders.

The insights derived from this research hold significant implications for various stakeholders. For FinTech companies, it provides strategic insights into the latest

cybersecurity trends and risk mitigation strategies. For regulators and policymakers, the findings can aid in designing robust cybersecurity frameworks to enhance digital financial security while fostering innovation. For technology providers, this study identifies key areas for cybersecurity advancements, including AI-driven fraud detection, zero-trust security models, and blockchain-based authentication mechanisms. Lastly, for the academic community, this research contributes to the growing body of literature on cybersecurity in FinTech, particularly in the context of digital financial ecosystems in developing economies. The study is structured to provide a comprehensive analysis of cybersecurity challenges in FinTech. The contextual background presents the key challenges that set the foundation for this research, followed by a literature review that examines existing theories and empirical findings on cybersecurity risks in financial technology. The methodology outlines the research approach, data collection techniques, and analytical frameworks used in this study. The results and discussion section presents findings on cybersecurity research trends and their implications for the financial sector, while the conclusion and recommendations offer actionable insights for industry stakeholders.

By addressing these critical aspects, this research seeks to bridge the gap between global knowledge and localized applications of cybersecurity strategies in FinTech. Drawing from foundational studies such as those by Arner et al. (2016) and Zetzsche et al. (2018), this study aims to provide a data-driven understanding of cybersecurity challenges, risk mitigation strategies, and emerging trends in financial technology. Through its findings, this research aspires to contribute to the development of secure, resilient, and innovative financial ecosystems, particularly in emerging economies where digital financial services are rapidly expanding.

Literature Review

This study aims to explore the cybersecurity challenges faced by FinTech firms, emphasizing the increasing complexity of cyber threats in digital financial services and the evolving security frameworks designed to mitigate them. As FinTech companies leverage technologies such as cloud computing, artificial intelligence (AI), blockchain, and open banking APIs, they also become prime targets for phishing attacks, ransomware, fraud, data breaches, and insider threats (Arner et al., 2016). Cybersecurity in FinTech is particularly crucial due to the sensitive nature of financial data and regulatory compliance requirements. Mishra & Kaushik (2023) highlight that while FinTech fosters financial inclusion and innovation, the interconnected nature of financial ecosystems creates vulnerabilities that cybercriminals exploit. The growing reliance on digital banking, mobile payments, and decentralized finance (DeFi) has expanded the attack surface for malicious actors (Shoetan et al., 2024). FinTech firms must navigate an increasingly complex security landscape, balancing technological innovation, regulatory compliance, and risk mitigation strategies (Zetzsche et al., 2018). Despite the implementation of advanced cybersecurity measures, data breaches, API vulnerabilities, smart contract exploits, and regulatory challenges remain persistent threats. The literature underscores the need for continuous improvement in cybersecurity frameworks to safeguard financial institutions and consumers from emerging threats.

Cybersecurity Threats in FinTech

A study by Arner, Barberis, and Buckley (2016) examined the cybersecurity risks associated with digital financial services, emphasizing that FinTech firms are highly vulnerable due to their reliance on cloud computing, mobile platforms, and open banking APIs**.** The research highlighted that the growing interconnectedness of digital finance ecosystems increases the likelihood of cyberattacks. The study recommended that FinTech firms adopt strong encryption, AI-driven fraud detection, and multi-factor authentication (MFA) to enhance cybersecurity resilience. Mishra and Kaushik (2023) explored major cybersecurity challenges faced by FinTech startups and digital banking platforms**,** identifying phishing attacks, identity theft, and malware infections as the most prevalent threats. The study suggested that regulatory compliance with GDPR, PSD2, and the U.S. Cybersecurity Framework plays a crucial role in strengthening cybersecurity defenses in FinTech.

Impact of Cybersecurity on Customer Trust and Satisfaction

Zetzsche et al. (2018) investigated the relationship between cybersecurity threats and consumer trust in FinTech services, emphasizing that security breaches negatively impact customer satisfaction and adoption rates. The study found that customers are more likely to abandon digital financial platforms if they perceive security risks, highlighting the need for FinTech firms to prioritize cybersecurity as a fundamental business strategy**.** Karim et al. (2022) analyzed the role of AI and machine learning in fraud detection, concluding that predictive analytics and real-time transaction monitoring significantly enhance cybersecurity in FinTech. The study found that FinTech firms leveraging AI-driven security measures reported lower fraud rates and higher customer trust levels**.**

Regulatory and Compliance Challenges

A study by Gurung and Shrestha (2020**)** explored the cybersecurity regulatory landscape for FinTech firms, identifying challenges such as inconsistent regulations, compliance costs, and jurisdictional differences**.** The research suggested that global regulatory bodies should develop harmonized cybersecurity policies to create a standardized security framework for digital financial services. The World Economic Forum (2021**)** conducted an analysis of cybersecurity regulations in Europe, the U.S., and Asia, concluding that compliance with international security standards such as ISO 27001, GDPR, and PSD2 **enhances** consumer confidence in FinTech. The study recommended that FinTech firms proactively adopt security best practices, conduct regular risk assessments, and implement robust incident response protocols**.**

Cybersecurity Technologies and Innovations in FinTech

Casey and Wong (2017) examined the role of blockchain technology in enhancing cybersecurity in financial services. The study found that blockchain's decentralized nature, immutability, and encryption features significantly reduce risks associated with fraud, unauthorized access, and transaction tampering**.** The findings suggested that FinTech firms should explore blockchain-based security solutions to enhance trust and transparency. Sharma et al. (2019) explored emerging cybersecurity solutions in FinTech, highlighting the adoption of biometric authentication, behavioral analytics, and zero-trust

architectures as critical advancements in financial security. The study emphasized that implementing multi-layered security protocols is essential for mitigating cybersecurity threats.

Cybersecurity Risks in Emerging Markets

A study by Hussin et al. (2024**)** investigated cybersecurity challenges in developing economies**,** finding that low digital literacy, weak regulatory frameworks, and inadequate security infrastructure contribute to higher cybersecurity risks in FinTech. The research emphasized the need for collaborative efforts between governments, financial institutions, and cybersecurity firms to enhance security measures and consumer awareness. Khanal (2023) examined cybersecurity vulnerabilities in mobile banking services in Nepal**,** concluding that factors such as poor encryption standards, lack of two-factor authentication (2FA), and phishing attacks remain significant threats. The study recommended that Nepalese FinTech firms adopt global security standards and conduct cybersecurity training programs to strengthen financial security.

Despite the growing body of literature on cybersecurity within the FinTech sector, several critical gaps remain unaddressed. First, existing studies predominantly focus on conceptual discussions, case analyses, or technology-specific risks such as blockchain vulnerabilities, API security, or cloud-based threats. While these works provide valuable insights, there is limited systematic and quantitative evaluation of how cybersecurity research in FinTech has evolved over time across global academic landscapes**.** A comprehensive bibliometric analysis that maps publication trends, key authors, influential works, and collaborative research networks is noticeably lacking. Second, past studies often treat cybersecurity in FinTech as a subset of broader digital finance or information security topics, resulting in fragmented understanding and dispersed findings**.** There is no consolidated assessment that integrates cybersecurity challenges specifically faced by FinTech firms across different technologies AI, blockchain, mobile platforms, open banking APIs and across different economic contexts.

Theoretical Frameworks in Cybersecurity Research

Venkatesh, Thong, and Xu (2012) introduced the Unified Theory of Acceptance and Use of Technology (UTAUT2**)** to explain how customers adopt cybersecurity measures in digital finance. The framework suggests that perceived security, ease of use, and trust are key factors influencing customer adoption of secure FinTech platforms. Zhao, Seibert, and Hills (2005) examined the role of self-efficacy in cybersecurity adoption**,** concluding that customers with higher digital literacy are more likely to adopt secure digital banking practices**.** The study recommended that FinTech firms focus on user education and cybersecurity awareness programs to reduce fraud risks and enhance consumer trust. The existing literature provides valuable insights into the cybersecurity challenges faced by FinTech firms and highlights the importance of regulatory compliance, technological advancements, and consumer awareness in mitigating cyber threats. However, there is a need for further bibliometric analysis of global research trends to assess how cybersecurity risks evolve over time and how FinTech firms can adopt data-driven security strategies to protect financial ecosystems.

Research Methods

This study employs a bibliometric analysis approach to examine global research trends on cybersecurity challenges faced by fintech firms. The research focuses on peer-reviewed articles, academic studies, and reports published in reputable databases such as Dimensions, Scopus, and Web of Science. The selection criteria prioritize recent publications from the last decade that specifically address cybersecurity risks, threat mitigation strategies, and regulatory frameworks in the fintech sector. To conduct the bibliometric analysis, specialized software tools such as VOSviewer and Biblioshiny (R programming package) will be used. Citation analysis will help identify the most influential studies and authors, while co-citation analysis will reveal interconnections between key research papers. Keyword frequency analysis will highlight dominant cybersecurity concerns and emerging trends in fintech. Additionally, network analysis will visually map collaborations between authors, institutions, and journals, offering insights into the research landscape.

Relevant articles were selected based on the following criteria:

- Keywords**:** ("cybersecurity" OR "cyber threats" OR "data breaches" OR "hacking" OR "fraud prevention") AND ("fintech" OR "financial technology" OR "digital banking" OR "payment systems")
- Document type: Peer-reviewed journal articles and conference papers
- Publication period: 2016–2025
- Open-access availability

The extracted data, formatted in CSV files, will be processed using bibliometric software to generate citation networks, thematic clusters, and keyword co-occurrence maps. The study will provide visual representations of research trends, influential contributors, and the evolution of cybersecurity challenges in fintech.

Ethical considerations will be strictly followed by ensuring transparency in data collection, proper citation of all sources, and objective analysis of research trends. The results of this study will offer valuable insights into how the global fintech industry is addressing cybersecurity threats and what gaps remain in existing research.

Findings

This section presents the bibliometric analysis of research on digital finance and customer satisfaction, covering publication trends, citation impact, key contributors, and thematic patterns.

Major Data

Table 1

Bibliometric Data

Category	Value
Timespan	2016-2025
Sources	240
Documents	311
Annual Growth Rate	34.43%

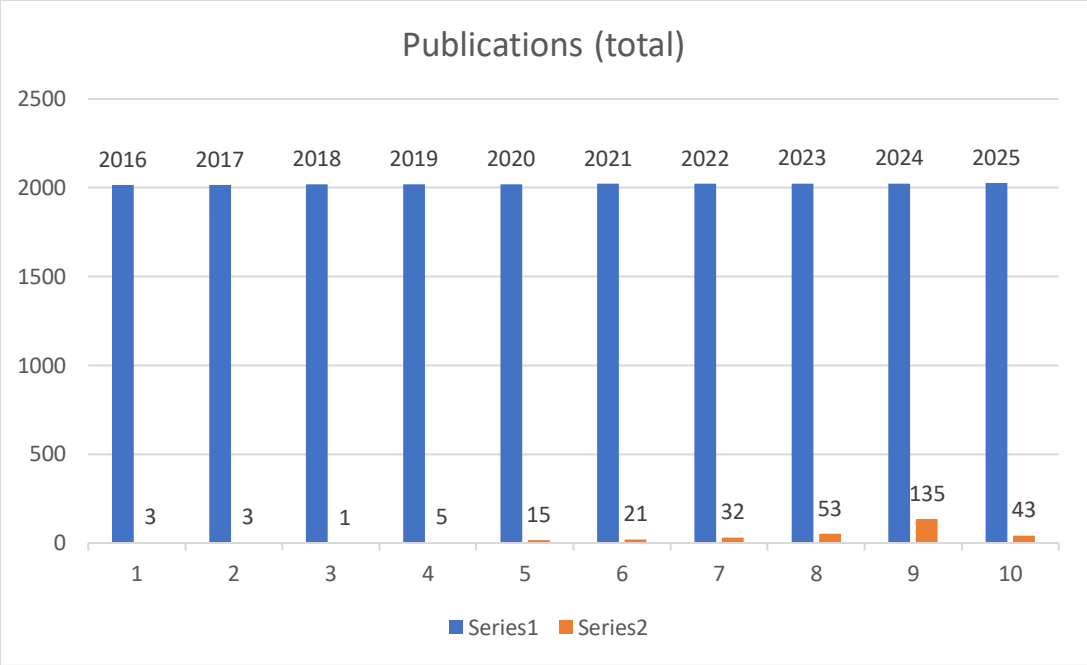
Authors	829
Authors of Single-Authored Docs	83
International Co-Authorship	8.039%
Co-Authors per Document	2.78
Author's Keywords (DE)	1
References	3744
Document Average Age	1.88 years
Average Citations per Document	7.621

The bibliometric analysis of digital finance and customer satisfaction spans from 2016 to 2024, covering nearly a decade of research growth. The 311 published documents across 240 sources suggest that research in this field is well-disseminated across multiple academic journals. A 34.43% annual growth rate highlights the increasing relevance of digital finance, likely driven by the rise of mobile banking, digital payments, and fintech innovations. The study identifies 829 authors, with most publications being co-authored, as only 83 documents are written by a single author. This indicates a strong culture of academic collaboration. However, international co-authorship is 8.039%, suggesting that while some studies involve global partnerships, there is still room for increased cross-border research efforts.

The average number of co-authors per document is 2.78, reinforcing that most studies are team-based. The 3744 references show a robust foundation of existing research supporting new findings. The document average age of 1.88 years suggests that most cited works are recent, reflecting the fast-changing nature of digital finance. Additionally, the average citation per document is 7.621, indicating that studies in this field have a notable academic impact.

Publication over the year

Figure 1
Publication over the year



This bar chart demonstrate the growth in publications on “Cybersecurity challenges faced by Fintech firms” from 2016 to 2025. Initially, the number of publications was minimal with only three article each in 2016 and 2017 and only one article in 2018. followed by a modest increase to five articles per year in 2019. This slow growth indicates limited research or awareness during the early adoption phase of cybersecurity in the fintech firms. However from 2020 onward the publications show a consistent and significant rise. There are 15 articles in 2020, 21 articles in 2021, and the growth accelerates in 2022 with 32 articles, reflecting growing interest and advancements in blockchain’s applications. In 2023, publications nearly double to 53, and by 2024 the figure leaps to 135 articles and 43 articles in 2025 highlighting the cybersecurity challenges faced by fintech firms.

Most relevant sources

Table 2

Most relevant sources

Sources	Articles
Finance & Accounting Research Journal	11
International Journal of Finance	11
Interantional Journal of Scientific Research in Engineering and Management	7
Interantional Journal of Scientific Research in Engineering and Management	7
Journal of Information Systems Engineering & Management	6
Journal of Infrastructure Policy and Development	5
Educational Administration Theory and Practice Journal	4

International Journal of Science and Research Archive	4
Economic Scope	3
Procedia Computer Science	3

This table lists the academic journals that have published the highest number of papers on Cybersecurity challenges faced by fintech firms.. Journals like *Finance & Accounting Research Journal*, *International Journal of Finance*, and *Interantional Journal of Scientific Research in Engineering and Management* appear frequently, suggesting that these are key platforms where research in this field is being published. Identifying these sources helps in understanding where the major academic discussions are taking place.

Most relevant Authors

Table 3
Most Relevant Authors

Authors	Articles	Articles Fractionalized
Adebimpe Bolatito Ige Abi	2	1.00
Adekunle Abiola Abdul Aaa	2	0.37
Al-Zaidi R	2	0.50
Albenjasim S	2	0.50
Aleksandrov A	2	1.50
Ali Mm	2	1.00
Anwuli Nkemchor Obiki-osafiele Ano	2	0.67
Awais M	2	0.45
Brus S	2	1.33
Dargahi T	2	0.50

This table highlights the authors who have contributed the most articles on cybersecurity challenges faced by fintech firms. Some authors have multiple publications in this area, indicating their expertise and influence in the field. The fractionalized article count accounts for co-authorship, meaning that if a paper has multiple authors, the contribution is divided among them. Recognizing these leading authors can help researchers identify key studies and potential collaborators.

Average Citations per Year

Table 4
Average Citations/year

Year	MeanTCperArt	N	MeanTCperYear	CitableYears
2016	0.00	2	0.00	10
2017	2.00	2	0.22	9
2019	14.33	3	2.05	7
2020	47.00	14	7.83	6
2021	34.06	18	6.81	5
2022	17.15	26	4.29	4
2023	4.49	43	1.50	3
2024	2.83	120	1.42	2
2025	0.03	39	0.03	1

The Table 4 presents data on citation metrics over a series of years, highlighting trends in research output and citation impact. The columns include: Year denotes the specific year for which the data is reported.

MeanTCperArt (Mean Total Citations per Artic column indicates the average number of citations received by articles published in each respective year. A higher value suggests that articles from that year have been more influential or impactful. For instance, 2020 shows a peak with an average of 47.00 citations per article.

N represents the number of articles published in that year. It provides context for the MeanTCperArt value. For example, in 2024, there were 120 articles published, but the MeanTCperArt dropped to 2.83, indicating a decline in the average impact of these articles.

MeanTCperYear (Mean Total Citations per Year): This metric reflects the average total citations received by all articles published in that year. It gives a broader view of how the research output from that year has been cited overall. The highest value is in 2020 with 7.83, suggesting significant recognition of the articles published during that period.

CitableYears indicates the number of years since the articles were published that can still be cited. For example, in 2016, articles could still be cited after 10 years, while those published in 2025 can only be cited for 1 year, reflecting their recency.

From 2016 to 2020, there was a notable increase in both MeanTCperArt and MeanTCperYear, peaking in 2020. This suggests that articles published during this time

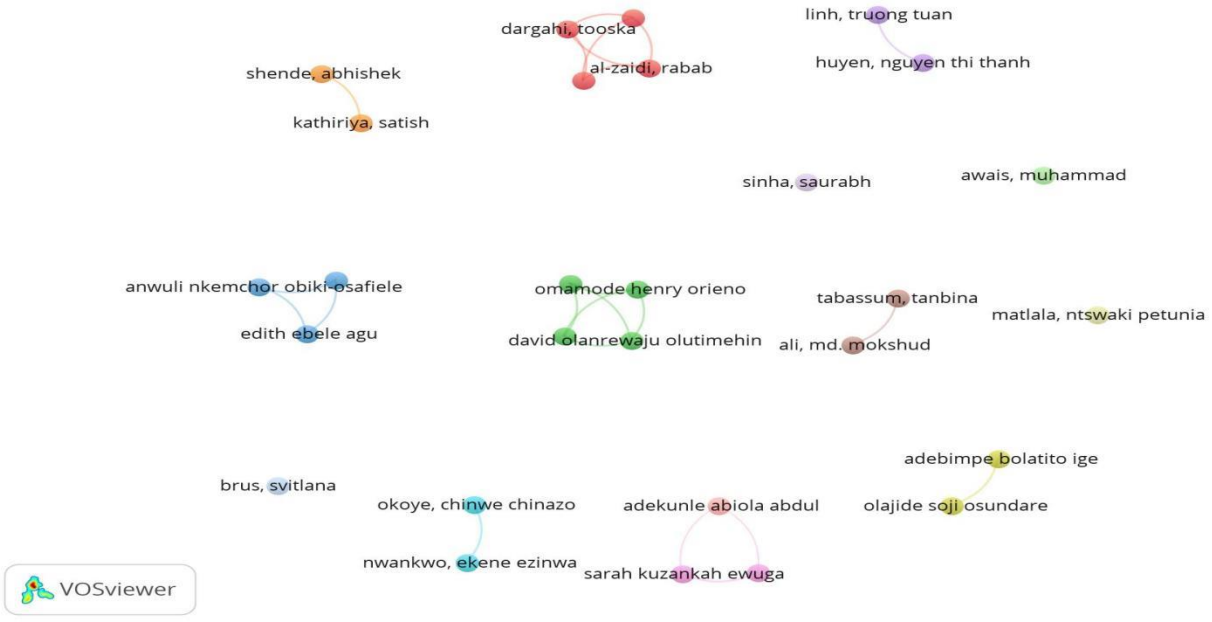
gained substantial recognition. After 2020, there is a decline in both metrics. For example, in 2023, the MeanTCperArt drops to 4.49, and in 2025, it falls further to 0.03, indicating a decrease in impact and recognition for more recent articles. The significant increase in N (number of articles) in 2024 to 120 does not correlate with a high MeanTCperArt, indicating a potential issue where more articles are being produced but with less impactful or less cited research. Articles published in more recent years tend to have lower citation counts due to their novelty and the time required for them to accumulate citations. This is reflected in the declining MeanTCperYear and MeanTCperArt values as we move towards 2025. Overall, the table illustrates the dynamics of academic publishing and citation trends, indicating periods of high impact and subsequent declines, as well as the challenges of maintaining citation relevance in a growing body of literature.

Co-authorship by authors

This figure zooms in on individual co-authorship patterns. It highlights which researchers frequently work together and how often they collaborate. If certain names appear repeatedly with multiple co-authors, it suggests they are leading research teams or are part of strong institutional collaborations. On the other hand, if some authors have only one or two collaborations, they may be working on specialized studies. Recognizing these patterns can help new researchers find potential mentors or partners in the field.

Figure 2

Co-authorship by Authors

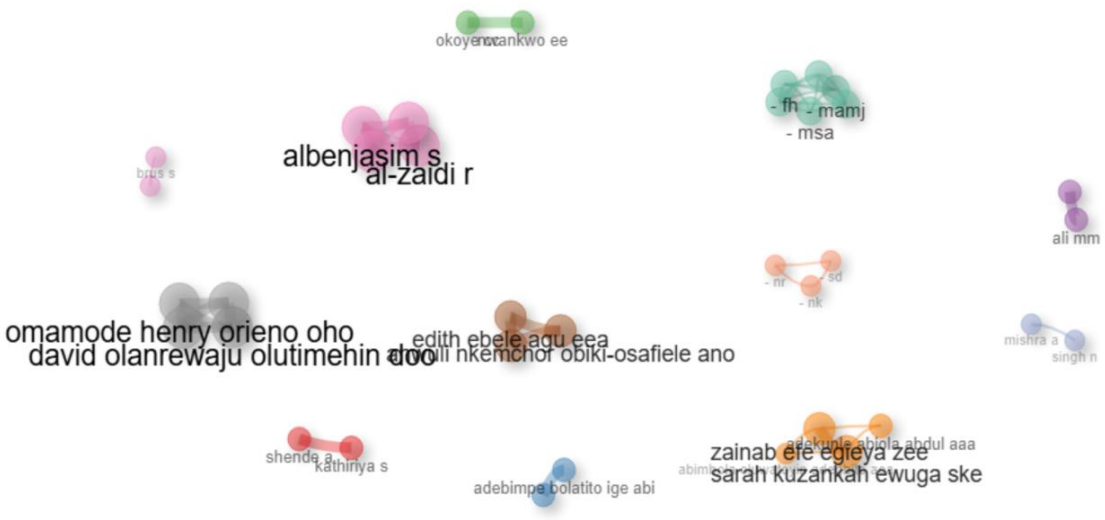


In the above figure, we can see prominent authors such as Dargahli Tooska, Al-Zaidi Rabab, and Omamode Henry Orieno appear as central figures in the network, reflecting

their significant contributions and frequent collaborations. The visualization highlights distinct clusters of authors working closely together, indicating specialized focus areas or institutional affiliations, particularly among authors like Anwuli Nkemchor Obiki-Osafiele and Edith Ebele Agu. Smaller collaborative groups, such as those involving Adekunkle Abiola Abdul and Olajide Soji Osundare, suggest the presence of niche research or localized efforts. This layout effectively illustrates the dynamics of collaboration and interconnectedness among researchers represented in the dataset.

Collaboration network

Figure 3
Collaboration Network

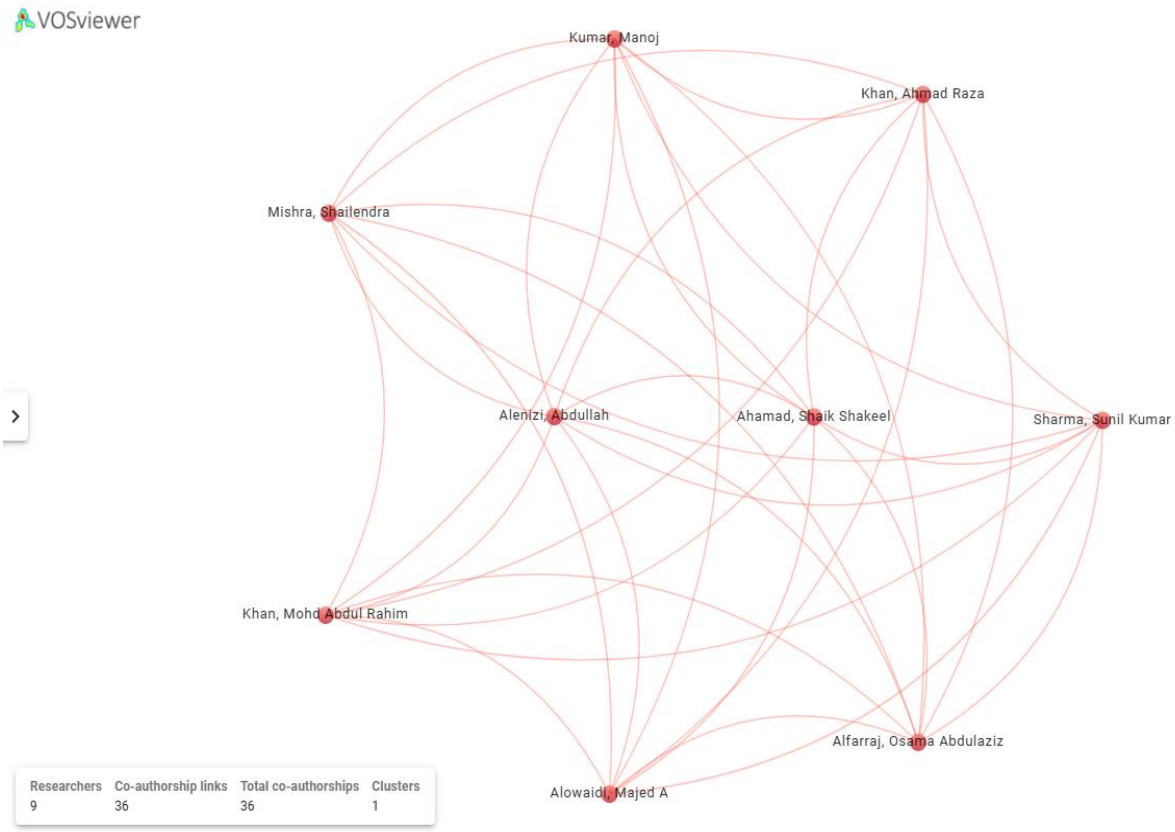


The figure represents a visualization of data, representing relationships or connections among various entities, authors or contributors in a certain field. Each labeled point corresponds to an individual, with their names displayed. The positioning and spacing between these points may indicate the strength or type of relationships, collaborations, or similarities between them.
In the above figure, we can see prominent authors such as Albenjasim S., Al-Zaidi R., and Omamode Henry Orieno Oho appear as central figures in the network, reflecting their significant contributions and frequent collaborations. The visualization also highlights distinct clusters of authors working closely together, indicating specialized focus areas or institutional affiliations. Additionally, smaller collaborative groups, such as those involving Zainab Ede Egleya Zee and Sarah Kuzankah Ewuga, suggest the presence of niche

research or localized efforts. This layout provides insights into the dynamics of collaboration and the interconnectedness of researchers within the represented dataset.

Co-authorship Analysis

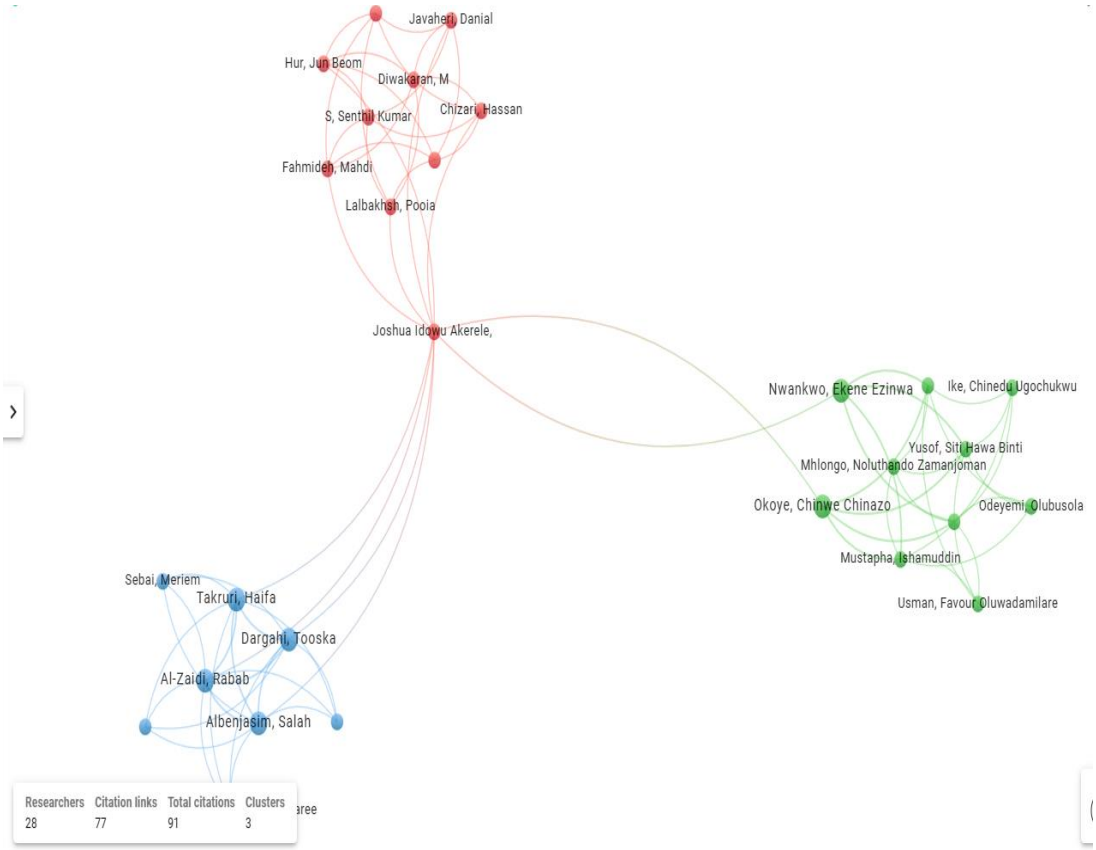
Figure 4
Co-authorship Analysis



In the above figure, we can see prominent authors such as Mishra Shaitendra, Kumar Manoj, and Khan Ahmad Raza appear as central figures in the network, reflecting their significant contributions and frequent collaborations. The visualization highlights a cohesive cluster of researchers, indicating a strong collaborative environment among the nine authors represented. Each line signifies co-authorship links, with a total of 36 connections demonstrating active partnerships within this group. Additionally, authors like Alenzi Abdullah and Alowaid Majed A contribute to the interconnectedness of this network, suggesting a unified focus on specific research areas. Overall, this layout effectively illustrates the dynamics of collaboration and the collective efforts of these researchers in their field.

Citation analysis

Figure 5
Citation Analysis



In the above figure, we can see prominent authors such as Joshua Idowu Akerele, Diwakaran M., and Javaheril Danial appear as central figures in the network, reflecting their significant contributions and frequent collaborations. The visualization highlights three distinct clusters of researchers, indicating specialized focus areas or institutional affiliations. The red cluster primarily features authors like Chizari Hassan and Lalbaksh Pooi, while the green cluster includes authors such as Nwankwo Ekene Ezinwa and Okoye Chinwe Chinazo, showcasing a strong collaborative environment among these researchers. Additionally, the blue cluster, which includes authors like Al-Zaidi Rabab and Takruli Haifa, demonstrates another active group within the network. With a total of 28 researchers and 77 citation links, this layout effectively illustrates the dynamics of collaboration and the interconnectedness of the researchers represented in the dataset.

Most cited countries

Table 5
Most Cited Countries

Country	TC	Average Article Citations
South Africa	591	197.00
USA	234	58.50
France	171	171.00
Jordan	153	51.00
India	143	14.30
Poland	118	118.00
Belgium	54	54.00
Korea	53	26.50
Australia	32	32.00
Malaysia	25	12.50

The Table 5 presents data on the total citations (TC) and average article citations for various countries, reflecting their academic impact and research output.

Total Citations (TC) column indicates the cumulative number of citations received by articles from each country. South Africa leads with 591 total citations, suggesting a strong presence in research that has garnered significant recognition. The USA follows with 234 citations, while France and Jordan have 171 and 153 citations, respectively.

Average Article Citations metric provides insight into the average number of citations per article published by researchers in each country. South Africa again stands out with an impressive average of 197 citations per article, indicating that its research is highly regarded. France also has a notable average of 171 citations, which complements its total citation count. In contrast, India shows a lower average of 14.30 citations per article, despite having 143 total citations, indicating a larger volume of articles with fewer citations.

Countries like Poland and Belgium have total citations that match their average article citations, suggesting consistency in the quality and impact of their research outputs. Malaysia and Australia have lower total citations and averages, reflecting less visibility or impact in the global research landscape compared to the top-performing countries. Overall, the table provides insights into the relative research performance of these countries, highlighting South Africa's dominance in both total and average article citations, while also revealing disparities among other nations in terms of research impact.

Discussion

The bibliometric analysis of cybersecurity challenges faced by FinTech firms reveals significant trends and insights into the evolving academic landscape surrounding this critical area. The study spans from 2016 to 2025, highlighting a robust annual growth rate of 34.43% in publications related to cybersecurity in FinTech. This surge indicates heightened awareness and urgency among researchers and practitioners regarding the cybersecurity vulnerabilities that accompany rapid digitization in financial services. The

publication trend illustrates a slow start in research output during the initial years (2016-2019), with only a handful of articles published. However, from 2020 onward, there was a dramatic increase in the number of publications, peaking at 135 articles in 2024. This spike can be attributed to several factors, including the increasing frequency of cyberattacks on financial institutions, regulatory changes, and advancements in technology that necessitated further exploration of cybersecurity measures. Notably, high-profile incidents such as the SolarWinds cyberattack and the Capital One data breach have likely catalyzed this academic interest, emphasizing the need for improved cybersecurity frameworks within the FinTech sector.

The analysis of authorship and collaboration reveals a strong culture of teamwork in this domain, with an average of 2.78 co-authors per document and a notable proportion of publications being co-authored. This collaborative approach is essential for addressing the multifaceted nature of cybersecurity challenges, as it brings together diverse expertise and perspectives. However, the relatively low percentage of international co-authorship (8.039%) suggests that there remains significant potential for enhancing global collaboration in cybersecurity research. Moreover, the citation analysis highlights key contributors to the field, showcasing authors who are leading the discourse on cybersecurity in FinTech. The average citations per document, which peaked in 2020, indicate that earlier works have had a substantial impact, while more recent publications may still be accumulating citations. This trend underscores the importance of giving time for newer research to establish itself within the academic community.

The bibliometric analysis also emphasizes regional disparities in research output and impact. South Africa emerged as a leader in total citations and average article citations, suggesting a strong academic focus and recognition of cybersecurity issues in the context of FinTech. In contrast, countries like India and Malaysia exhibit lower citation metrics, indicating potential gaps in research output or impact. This disparity highlights the need for emerging economies to bolster their cybersecurity research initiatives to keep pace with global developments.

Conclusion and Implications

This bibliometric analysis provides valuable insights into the current state of research on cybersecurity challenges faced by FinTech firms. The findings underscore the rapid evolution of the cybersecurity landscape as it pertains to financial technology, driven by both technological advancements and increasing threats. The significant rise in publications reflects a growing recognition of the vulnerabilities inherent in digital finance, necessitating ongoing research and collaboration across disciplines. The results emphasize the necessity for FinTech companies, regulators, and policymakers to prioritize cybersecurity as an integral component of their operational strategies. As the industry continues to advance, stakeholders must work together to develop comprehensive cybersecurity frameworks that not only address existing threats but also anticipate future challenges. This study contributes to the academic discourse on cybersecurity in FinTech, bridging the gap between theoretical understanding and practical application. It serves as a call to action for increased research efforts, particularly in developing economies, to enhance cybersecurity resilience in financial ecosystems. Future research should aim to explore specific case studies, develop standardized

practices, and foster international collaborations to create a more secure digital financial landscape.

Acknowledgment

The authors would like to thank stakeholders who took advantage of the chance to voluntarily participate in this study. The authors would also like to thank everyone and all sources that have contributed in various ways and improved the work.

Conflict of Interest

The Authors declare that there is no conflict of interest.

Funding

There was no external source of funding for the research.

References

Casey, M. J., & Wong, P. (2017). Global blockchain technology ecosystem: Future outlook. *Journal of Financial Transformation,* 45, 41-49.

Deng, Q., & Qing, Y. (2020). Regulatory compliance in fintech: Challenges and strategies. *Financial Stability Review, 24(*1), 101-115.

Gupta, A., Kumar, A., & Sharma, A. (2018). Open banking: Opportunities and challenges in cybersecurity. *Journal of Financial Services Marketing, 23*(1), 39-52. https://doi.org/10.1057/s41264-018-0021-4

Hussin, M. N., & Ahmed, K. (2024). Cybersecurity risks in developing economies: A focus on fintech. *International Journal of Emerging Markets, 19*(3), 456-475. https://doi.org/10.1108/IJOEM-01-2023-0154

Karim, M. R., Miah, M. S., & Hossain, M. M. (2022). Leveraging AI for enhanced cybersecurity in fintech: A systematic review. *Journal of Information Systems Security, 18*(1), 23-42.

Khanal, R. (2023). Cybersecurity vulnerabilities in mobile banking services in Nepal. *Asian Journal of Business and Management Studies, 14*(1), 22-30.

Miah, M. S., Ali, M. M., & Rahman, M. M. (2023). Ransomware-as-a-service: Implications for financial institutions. *Journal of Cybersecurity Technology, 7*(2), 113-130. https://doi.org/10.1080/23742917.2023.2175689

Mishra, S., & Kaushik, V. (2023). Cybersecurity challenges in fintech startups: A comprehensive analysis. *International Journal of Finance & Accounting, 12*(2), 35-50. https://doi.org/10.11648/j.ijfa.20231202.13

Refernces Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The emerging role of fintech in the financial services industry. *Journal of Financial Regulation and Compliance, 24*(1), 1-17. https://doi.org/10.1108/JFRC-03-2016-0024

Sharma, S., Singh, R., & Gupta, S. (2019). Emerging cybersecurity solutions in fintech: Biometric authentication and beyond. *International Journal of Computer Applications, 178*(20), 1-8. https://doi.org/10.5120/ijca2019918310

Shoetan, M., & Mhlanga, D. (2024). Cyber threats in the age of digital finance: *An empirical study. Journal of Financial Crime, 31*(2), 123-144. https://doi.org/10.1108/JFC-10-2021-0145

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 13*(5), 392-414.

World Economic Forum. (2021). The Global Cybersecurity Outlook 2021. Retrieved from https://www.weforum.org/reports/global-cybersecurity-outlook-2021

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The rise of fintech: A new era of financial services. European Banking Institute Working Paper Series, No. 2018/02. https://doi.org/10.2139/ssrn.3091290

Zhao, Y., Seibert, S. E., & Hills, G. E. (2005). The role of self-efficacy in the adoption of cybersecurity measures. *Computers & Security, 24*(4), 319-331. https://doi.org/10.1016/j.cose.2005.02.005

Authors' Bio

Rakshya Bhandari is affiliated with Nepal Commerce Campus and focuses her research on FinTech, cybersecurity, and emerging digital financial systems. Her academic interests particularly explore cybersecurity challenges, technological innovation, and the evolving risk landscape within modern financial services.

Note: The authors acknowledge the use of AI-assisted tools (such as Quillbot and ChatGPT) strictly for editing language, improving readability, and grammar checking. No AI tools were used for data analysis, interpretation, or the creation of original scientific content. The authors take full responsibility for the accuracy and integrity of the manuscript.