Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 6 Issue 1 (2026)

From Insurance to Cyber Insurance: A Longitudinal Bibliometric Trend Analysis Using Vosviewer and Biblioshiny

Dr. Neha Gulati[1], Isha Negi[2]*

[1]Assistant Professor, University Business School, Panjab University, Chandigarh, India

[2]*Research Scholar, University Business School, Panjab University, Chandigarh, India

***Corresponding author:** Isha Negi

*Email ID: ishanegi.ubs@gmail.com

Abstract

The rapid digitalization of economies and escalation of cyber threats have transformed the global risk landscape, driving the evolution of traditional insurance into specialized **Cyber Insurance**. Understanding this intellectual progression is essential for grounding future theoretical and empirical enquiries into cyber-risk management and adoption behavior. This study conducts a **longitudinal bibliometric trend analysis** to map the conceptual structure, thematic evolution, and collaborative dynamics of Cyber Insurance research. Data retrieved from the **Scopus database** in **May, 2025** and **September, 2025** provided a list of **238** and **267** published journal articles. **VOSviewer** and **Biblioshiny** were employed to visualize citation networks, author influence, and thematic clusters. Findings indicate a sharp increase in scholarly output after 2015, underscoring Cyber Insurance's growing prominence as a risk-transfer mechanism in the digital economy. *The Geneva Papers on Risk and Insurance* emerged as the leading source, with **Biener et al. (2015)** and **Eling, M. (2016)** identified as prominent authors. Thematic mapping revealed two dominant clusters, **risk management/cybersecurity** and **insurance/economics/security of data** with Cyber Insurance acting as a central link connecting both clusters. Emerging themes such as *AI-driven risk modeling, data protection,* and *technology readiness* demonstrate the domain's interdisciplinary expansion. The study provides a comprehensive knowledge framework to inform future research on behavioral and technological determinants of Cyber Insurance adoption.

Keywords: *Bibliometric Analysis; Cyber Insurance; Cybersecurity; Data Security; Decision Support System; Data Security; Information System; Longitudinal Study; Risk Management*

1. Introduction

Cybersecurity is a critical concern in today's digital world, with cyberattacks posing significant threats to businesses and individuals alike (Nobanee et al., 2023a). The pervasive use of computer systems and digital services, amplified by COVID-19 pandemic, has led to a greater exposure to risks such as ransomware, online scams, data breaches and online abuse (Jain et al., 2025). In addition, other adverse events like global warming and severe warfare also pose threats to organizational and ecosystem data protection (Singh et al., 2025). Cyber threats are real and they target individuals as well (Abramova et al., 2023). According to UK crime statistics, individuals were more severely impacted by cybercrimes than organizations during COVID-19 (Schutz et al., 2023). Cyberattacks have been identified as a primary concern for both government and private sector, contributing to 39% of the overall risk perception as highlighted in the Global Risk Report 2024, thus making cybersecurity a critical area of focus (World Economic Forum, 2024).

Increased access to the Internet makes individuals vulnerable to cyberattacks (Fenech et al., 2024). As the Internet and smart technology proliferate, cyberattacks are also changing in kind (Cremer et al., 2022). Today, supply chain assaults, ransomware, malware, cryptojacking, business email compromise, and other advanced cyberthreats of high severity are recurrent (Tsohou et al., 2023). Cyberthreats have consequences comparable to those of traditional terrorism (Abramova et al., 2023). Strategies to mitigate these risks include using antivirus, software, to lower the chances of falling victim to cybercrime (Abramova et al., 2023). However, these threats cannot be entirely eliminated through technical mitigations alone; thus, making response strategies like Cyber Insurance (CI) crucial for managing the financial consequences of cyber attacks (Jain et al., 2025). CI has emerged as a vital tool for reducing the financial risks associated with the cyber threats (Nobanee et al., 2023).

To increase stakeholder resilience; cybersecurity necessitates a robust insurance market and an efficient risk transfer regime (Cremer et al., 2024). The negative effects of cybercrimes have pushed both individuals and businesses to look into ways like CI to reduce cyber risk (McGregor et al., 2024). CI has become an essential risk management tactic (Adriko & Nurse, 2024a). "Cyber insurance, also known as cyber risk or cyber liability insurance, is a type of insurance coverage intended to shield a person or company from online dangers like hacking, data breaches, and cyberattacks" (Adriko & Nurse, 2024b). Its use as a risk management tool is expanding with the goal of transferring cyber risks to a third party in order to protect from monetary losses (Nobanee et al., 2023). CI is a developing market for the insurance industry due to the growing number of connected devices and the extensive availability of the Internet (Schutz et al., 2023). In addition to improving the capacities and efficiency of urban energy systems, the spread of information and communication technologies (ICTs) in smart cities has also brought serious cyberthreats that could

jeopardise these systems (Zhao et al., 2024). Furthermore, a growing number of Internet of Things (IoT) devices are being used in households, giving rise to the concept of "smart homes". Though making our daily lives more convenient, they also increase the risk of cyberattacks. The need for smart home cyber insurance has been rising quickly in order to reduce these risks (Zhang et al., 2024). The primary motivations for purchasing CI also include business interruption, cyber liability, and cyber extortion coverage (McGregor et al., 2024b). All this has helped the industry to reach a premium of US$7 billion in 2022 and a 15% compound annual growth rate by 2025.

Premiums in this sector are expected to reach US$22 billion (McGregor et al., 2024a). “The global CI market was valued at US$4.85 billion in 2018 by the international market research firm Allied Market Research, and it is projected to grow to US$28.60 billion by 2026” (Kshetri, 2020). The market for CI is new but growing quickly. CI is a nascent form of insurance in the digital economy. Several factors contribute to its continuous rise in demand, including the constantly changing and growing cyberthreat landscape, widespread media coverage of serious cyber incidents, implementation of stricter laws, and growing corporate awareness of their increased reliance on information technology (Zeller & Scherer, 2023). Research in this area has expanded significantly, with a notable increase in publications since 2009, indicating a heightened academic and industrial interest in the importance of CI (Nobanee et al., 2023a). Growing body of literature underscores the increasing importance of understanding and managing cyber risks through effective insurance strategies (Nobanee et al., 2023a).

However, insurers face a significant issue in effectively forecasting the future of client cyber risk due to the paucity of historical cyber threat data (McGregor et al., 2024a). Market for CI has grown rapidly in recent years, but insurance companies in this sector still face a number of obstacles, including lack of data, lack of automated tasks, a rise in fraudulent claims from legitimate policyholders, attackers posing as legitimate policyholders, and the fact that insurance companies are frequently the targets of cybersecurity attacks because of the volume of data they store (Farao, 2024). Also, standardization and clear language in the policies are necessary for consumers to comprehend CI (Schutz et al., 2023a). Policy definitions and terminology are not standardized and pose confusion for scholars, policymakers, and prospective clients (Nobanee et al., 2023b).

To address this gap, Cyber insurance is reviewed bibliometrically in the present study. The query formulated using keywords "cyber insurance" “OR” "cyber-insurance" “OR” "cybersecurity insurance" “OR” "cyber risk insurance" “OR” "personal cyber insurance" “OR” "cloud insurance" “OR” "cyber liability insurance" was executed on Scopus on 28th May, 2025 and on 29th September, 2025. It extracted 503 articles in May and 588 articles in September for the bibliometric study. Such a study helps to address the current state of intellectual structure of a discipline by summarizing the extensive bibliometric data. It is applied when the amount of data is extensive and wide-ranging, making manual data assessment challenging (Nobanee et al., 2025). Through an examination of publication patterns, co-authorship networks, thematic evolution, and citation impact, the longitudinal study aims to provide a comprehensive bibliometric analysis of the academic work published on CI with the goal of mapping the field's knowledge structure across two distinct time points and offering insights for future academic research and policy development, tracking the evolution, growth as well as revealing trends and shifts in the intellectual landscape of Cyber Insurance.

2. Methodology

The use of quantitative methods on bibliometric data like units of publication, citations, etc. is referred to as bibliometric methodology (Broadus, 1987). “It is a measurement analysis that characterizes all documents on a certain subject in terms of citations, communication, quantity, quality, productivity, and intellectual growth” (Nobanee et al., 2023). The primary goal is to identify trends, map the collaborative networks, pinpoint influential work, and uncover research gaps (Xu et al., 2017). Through the visual representation of citation and co-citation networks; bibliometric analysis enables the identification of foundational intellectual structures and emerging research trajectories that may have been overlooked in conventional literature reviews (Alaassar et al., 2025). It is particularly useful when reviewing a large volume of literature as manually reviewing poses a big challenge.

Present work undertakes a bibliometric study of the literature on Cyber Insurance by mapping the intellectual structure and identifying key research trends. By systematically reviewing published work from 2003 to 2025, goal of the study is to present a thorough summary of the field; highlighting influential authors, key publications, and the evolution of thematic clusters within Cyber Insurance research. For this it employs quantitative measurement technique to evaluate various subjects and to create connections between them. The study uses Scopus as a database for extracting documents. These documents are analyzed using VOSviewer and Biblioshiny. Researchers often select Scopus over alternative databases because of its extensive coverage of high-quality journals from varied publishers such as Wiley, Sage, Springer, and Cambridge University Press (Martín-Martín et al., 2018).

Studies comparing major scholarly databases have highlighted that Scopus offers a balanced combination of breadth and indexing rigor, making it particularly valuable to map research landscapes and uncover scholarly networks (Falagas et al., 2008). The selection of precise keywords and the construction of an effective search query are critical steps in conducting bibliometric analysis, as inappropriate keyword choices lead to the retrieval of irrelevant documents. To

achieve comprehensive coverage; synonyms and related terms were identified from the existing literature on cyber insurance. These keywords included “cyber insurance”, “cyber-insurance”, “cybersecurity insurance”, “cyber risk insurance”, “personal cyber insurance”, “cloud insurance”, and “cyber liability insurance”. After finalizing the keywords, individual search queries were executed independently on the Scopus database on 28th May 2025 and on 29th September, 2025 to observe the retrieved documents. The keywords were then combined using the Boolean operator “OR” to formulate the final search query. The Boolean operator “OR” was used to broaden the scope of the search and retrieve a diverse range of relevant publications. This approach ensures that all synonyms and related phrases linked to the theme are included, thereby providing a vast coverage of the research domain. The inclusion of variations in spelling and phrasing is essential to uncover all relevant literature, especially in an interdisciplinary field like CI, where authors may use varying terminologies from different domains. Analysis was restricted to articles published in journals because these are recognized as validated and reliable sources of scholarly knowledge, frequently used in management-focused bibliometric reviews (Danvila-del-Valle et al., 2019). Additionally, only articles in English language were included, reflecting both practical language considerations and common practices in prior bibliometric studies (Mongeon & Paul-Hus, 2016). The initial search resulted in 503 documents as on 28th May, 2025 and 588 documents as on 29th September, 2025. After applying inclusion and exclusion criteria, only English-language journal articles were selected, reducing the corpus to 242 documents for May, 2025 and 273 for September, 2025. Subsequently, the retrieved documents were exported in a compatible format (e.g., CSV or RIS) and data cleaning was conducted manually to remove duplicates and irrelevant entries, which involved identifying and removing incomplete records or those lacking sufficient bibliographic information and a final corpus of 238 articles for May, 2025 and 267 articles for September,2025 as presented in Table 1 were retained for bibliometric analysis. The study uses VOSviewer and Biblioshiny to leverage their complementary strengths in bibliometric analysis. VOSviewer is used for advanced network visualization and Biblioshiny presents a user-friendly interface with diverse analytical features. This two-pronged strategy guarantees a more thorough and perceptive investigation of the subject “Cyber Insurance”.

Table 1: Search Query

Title	**Description**	**Documents Retrieved**
Search query	"cyber insurance" “OR” "cyber-insurance" “OR” "cybersecurity insurance" “OR” "cyber risk insurance" “OR” "personal cyber insurance" “OR” "cloudinsurance" “OR” "cyber liability insurance"	
Search query execution date	28th May, 2025 29th September, 2025	238 267
Research Publication	2003-2025	
Subject area	All subject areas	
Source type	Journal articles	
Language	English	

Source: Researchers’ compilation

3. Results and Discussion

3.1 Number of publications based on year

Since 2003, there has been a notable upsurge in the number of research articles published on the theme related to CI. This demonstrates the widespread interest among researchers in CI and thereby helps to present a strategy for preventing cyber assaults (Nobanee et al., 2023).

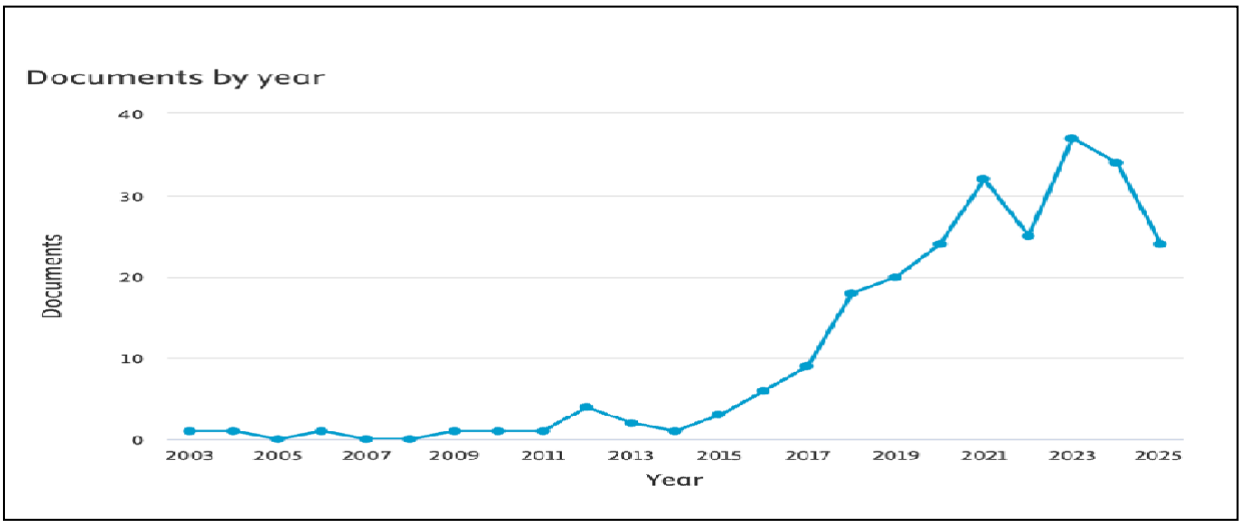

Figure 1: Document published by year

Source: Researchers' compilation

The quantity of research articles on CI is clearly on the rise, especially from 2015 onwards, with a considerable uptick from 2018 (Adriko & Nurse, 2024b). Similar trends are presented in Figure 1. It suggests that as cyber threats have become more prevalent and sophisticated, thus directing the focus on CI as a critical risk management tool (Nobanee et al., 2023). This highlights the increasing acknowledgement of the importance of CI. This surge in research indicates a widespread acknowledgement of its role in helping organizations protect themselves against the financial repercussions of cyberattacks. The visualization of publication trends, clearly illustrates this upward trajectory, with notable increase observed from around 2015 and a peak in publication activity from 2018 onwards (Nobanee et al., 2023). This growing academic interest is further evidenced by the clear upward trend in publications from approximately 2015, peaking around 2019, a period marked by escalating cyber threats and a greater demand for risk transfer mechanisms (Tsohou et al., 2023).

3.1 Analysis of Citations and Bibliographic Coupling

Bibliographic coupling refers to the relationship between two documents that cite one or more of the same work (Nobanee et al., 2023a). Thus, creating a link based on shared outward citations rather than incoming citations. The strength of this coupling is determined by the number of references they share. A higher coupling strength is typically interpreted as indicating greater topical or thematic similarity between the documents (Holmberg, 2016).

3.1.1 Top published documents on Cyber Insurance

The most cited work on CI as depicted by VOS Viewer as on September, 2025 is presented in Table 2.1 and the bibliographic coupling is illustrated in Figure 2. Work by Biener et al. (2015) is the most referred source with 227 citations, where majority of the citations are from United States (54), followed by Switzerland (31) and Italy (24), implying that a large number of researchers have utilised this source for augmenting their research.

From India there are 6 citations to the work by Beiner et al.(2015) Several Indian-authored studies including works on cybercrime legislation, AI-driven actuarial models, digital disruption in the insurance value chain, and systemic cyber-risk in IoT contexts all cite the seminal contribution of Biener et al. (2015) on the insurability of cyber risk. Although these Indian studies differ in orientation ranging from legal and regulatory frameworks to technological innovation, market dynamics, and quantitative risk modelling, but their reliance on the study by Biener et al. (2015) as a foundational reference, couple them together in a bibliometric map. The second highly cited work is of Cremer et al. (2022) with 210 citations.

Table 2.1: Most Cited Published Work as in September, 2025

S. No.	Documents	Citations
1	Biener et al. (2015)	227
2	Cremer et al. (2022)	210
3	Romanosky et al. (2019)	207
4	Radanleiv (2018)	127
5	Mukhopadhyay (2013)	126

Source: Researchers' compilation

Table 2.2: Most Cited Published Work as in May, 2025

S. No.	Documents	Citations
1	Biener et al. (2015)	215
2	Romanosky et al. (2019)	183
3	Cremer et al. (2022)	148
4	Hoang (2017)	141
5	Mukhopadhyay (2013)	117

Source: Researchers' compilation

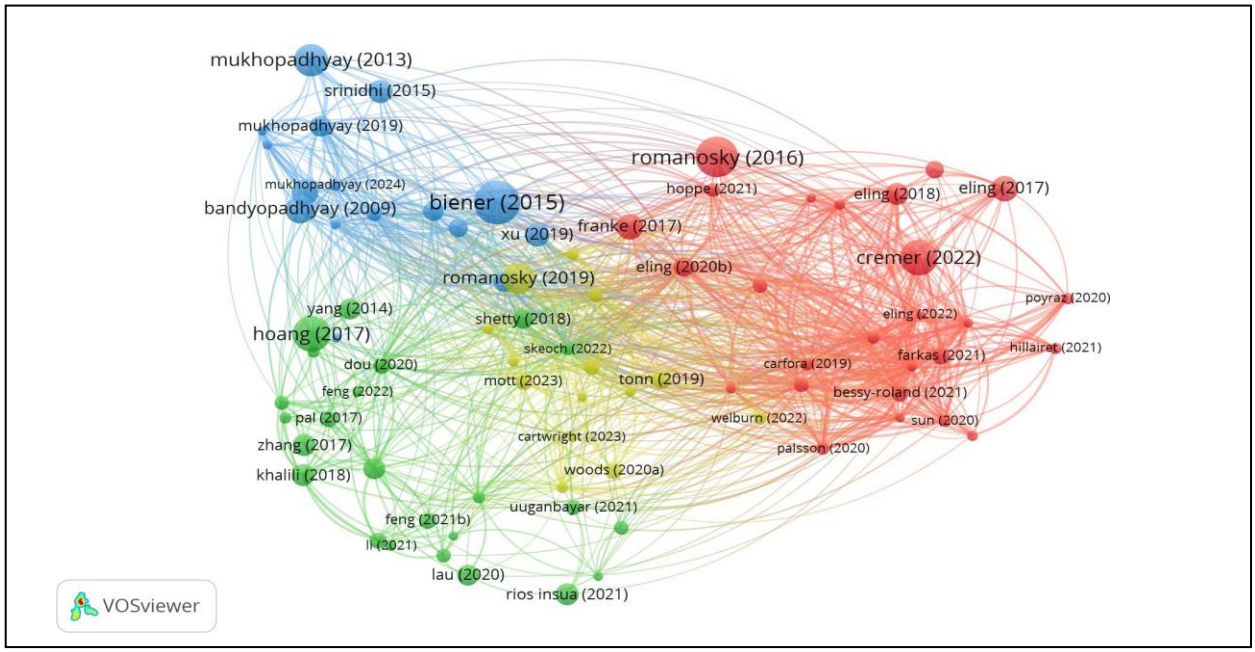

Figure 2: Documents by citation

Source: Researchers' compilation

The temporal analysis as in September 2025 as shown in Table 2.1 shows an increase in citation counts across almost all leading documents compared to Table 2.2 that presents citations as in May, 2025. Citations of Biener et al. (2015) have increased from 215 to 227 citations. This demonstrates the growing influence of foundational work on CI over a four-month period from May to September, 2025. This consistent increase in the number of citations reflects the rapid accumulation of scholarly attention towards CI as a domain.

From the Indian perspective, the steady referencing of Biener et al. (2015) and Mukhopadhyay (2013) underscores integration of global literature into Indian context-specific studies, especially in risk modelling and cybercrime legislation. This trend suggests that Indian research is both consuming and contributing to the global discourse.

3.1.2 Leading Sources

Table 3.1 presents the leading journals with highest published work on "Cyber Insurance" as on September, 2025. "The Geneva Paper on Risk and Insurance: Issues and Practice" remains the topmost journal with 15 articles published on "Cyber Insurance". This journal from Switzerland examines themes such as the insurability of cyber risks in global markets by Biener et al. (2015) and the role of CI in shaping ransomware payment decisions by Cartwright et al. (2023).

Table 3.1: Leading Journals on Cyber Insurance as in September, 2025

S.	Source	No.of	Citations
1	"Geneva Papers on Risk and Insurance: Issues and Practice"	15	686
2	"Computer and Security"	13	218
3	"Risks"	8	38
4	"Journal of Cybersecurity"	7	354
5	"Computer fraud and security"	7	10

Source: Researchers' Compilation

Table 3.2: Leading Journals on Cyber Insurance as in May, 2025

S.	Source	No.of	Citations
1	"Geneva Papers on Risk and Insurance: Issues and Practice"	15	574
2	"Computer and Security"	12	188
3	"Journal of Cybersecurity"	7	312
4	"Risks"	7	30
5	"Computer fraud and security"	7	8

Source: Researchers' Compilation

Recent contributions extend to optimal contract design for risk mitigation services by Zeller & Scherer (2023) and the systematic review of cyber risk data availability by (Cremer et al., 2022). Collectively, these studies demonstrate that the journal is not only analyzing the theoretical insurability of cyber risk but also engages with practical concerns of pricing, contract structures, market adoption, and systemic vulnerabilities. Thus, it acts as a central hub for advancing both the theoretical and applied understanding of how insurance markets can adapt to the evolving landscape of cyber threats.

VOSviewer Analysis of the top journals by citation counts as on September, 2025 is shown in Table 4.1, Figure 3 and as in May, 2025 in Table 4.2.

Table 4.1: Leading journals sorted by citations as in September, 2025

S. No.	Source	No.of Documents	Citations
1	"Geneva Papers on Risk and Insurance: Issues and Practice"	15	686
2	"Journal of cybersecurity"	7	354
3	"Insurance: mathematics and economics"	6	223
4	"Computers and Security"	13	218
5	"IEEE Transactions on Information Forensics and Security"	5	167

Source: Researchers' Compilation

Table 4.2: Leading journals sorted by citations as in May, 2025

S. No.	Source	No.of Documents	Citations
1	"Geneva Papers on Risk and Insurance: Issues and Practice"	15	574
2	"Journal of cybersecurity"	7	312
3	"Insurance: mathematics and economics"	6	191
4	"Computers and Security"	12	188
5	"IEEE Transactions on Information Forensics and Security"	5	160

Source: Researchers' Compilation

It highlights that the top journal in terms of citations is "Geneva Paper on Risk and Insurance: Issues and Practice" with 686 citations as in September, 2025 and 574 citations as in May, 2025.

"Insurability of cyber risk: An empirical analysis" by Biener et al. (2015), is the most cited article in the journal, followed by "Cyber risk and cybersecurity: a systematic review of data availability" by (Cremer et al,. 2022).

Citation counts have increased across almost all journals: "Insurance: Mathematics and Economics" from 191 to 223 and "Computers and Security" from 188 to 218. This signals that established journals are gaining more attention, further concentrating influence. This reflects both an expansion in volume and intensification in influence. Bibliometrically, this shows that the journals are consolidating their hubs of authority and there is no change in the ranking of these journals as shown in Table 4.1 and 4.2. For India, identifying such leading journals provides a roadmap for scholars to strategically target publications that maximize international visibility and policy relevance.

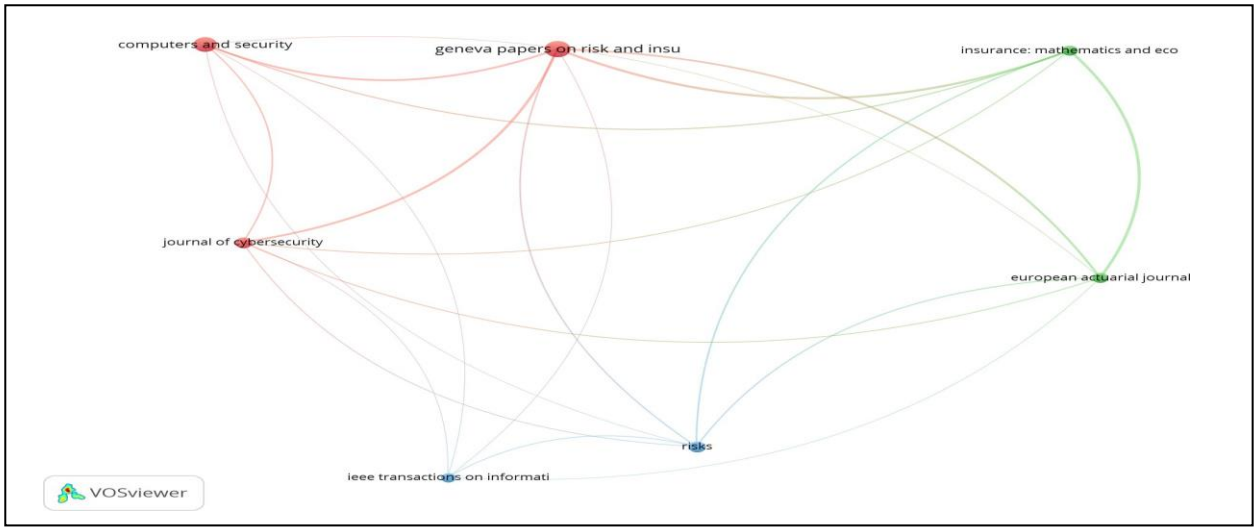

Figure 3: Top Journals

Source: Researchers' compilation

3.1.3 Leading Authors

This section highlights the highly influential authors in the domain as indicated by published document count and number of citations. Leading author "Eling, M." has contributed eleven research articles as in September, 2025 as compared to eight research articles as in May, 2025. "Niyato" has also been the prime author for their study thus, proving a consistent productivity of in the domain of CI in Singapore (Nobanee et al., 2023a). Table 5.2 and Figure 4 lists the top authors working in the domain of CI. The Indian author "Mukhopadhyay" has contributed seven published articles in the domain of CI. The work on, " Cyber-risk decision models: To insure IT or not?" (Mukhopadhyay et al., 2013), "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance" (Mukhopadhyay et al., 2019), and "A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks" Biswas et al., (2024) are extensively cited.

Table 5.1: Contribution by leading authors as in September, 2025

S. No.	Author	No. of Documents	Citations
1	"Eling, M."	11	641
2	"Niyato, D."	9	310
3	"Woods, Daniel W."	9	135
4	"Wang, P."	8	274
5	"Mukhopadhyay"	7	297

Source: Researchers' compilation

Table 5.2: Contribution by leading authors as in September as in May, 2025

S. No.	Author	No. of Documents	Citations
1	"Niyato, D."	8	275
2	"Eling, M."	8	431
3	"Wang, P."	7	262
4	"Mukhopadhyay"	7	231
5	"Wang, P."	7	152

Source: Researchers' compilation

These studies highlight India's contribution to the global discourse on CI, particularly in developing risk assessment frameworks, decision models for insurability, and statistical/machine-learning–based approaches to cyber risk prediction. This places Indian research, led by Mukhopadhyay and his collaborators, at a significant position in advancing both the theoretical and applied dimensions of cyber risk modelling and insurance solutions with drastic increase of 66 citations from 231 to 297 in the span of four months.

The order of influence of authors shifted slightly as shown in Table 5.1 and 5.2. Eling's citations overtook Niyato's, while Mukhopadhyay's citations rose from 231 to 297. This illustrates how temporal bibliometrics capture the fluidity of author influence. For India, Mukhopadhyay's increasing citations demonstrate the growing weight of Indian-origin research in shaping global discourse, offering a role model for young Indian scholars to scale their work internationally.

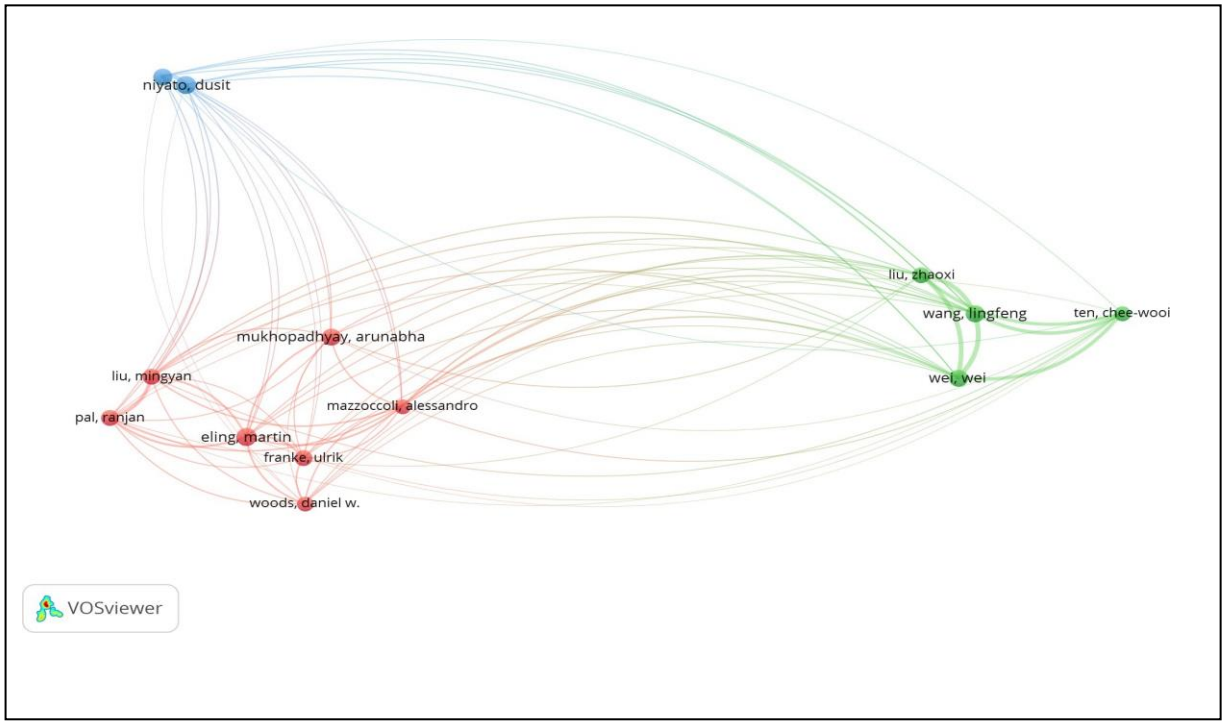

Figure 4: Top Authors by number of documents

Source: Researchers' compilation

3.1.4 Leading Organizations

Indian Institute of Management, Lucknow has contributed seven documents with 274 citations as shown in Table 6.1. This surpasses global leaders like Oxford and St. Gallen, thus highlighting increasing influence of Indian research in the area of CI as in September, 2025 is illustrated in Table 6.1. This is highly significant bibliometrically as India's institutional presence is now visible in the global citation network (Table 6.1) which was earlier dominated by western organizations as in May, 2025 (Table 6.2). This not only validates India's contributions but also highlights opportunities for expanding institutional collaborations with top-ranked global universities.

Table 6.1: Leading organizations as in September, 2025

S. No.	Organization Name	No. of Documents	Citations
1	"Collegeof Engineering and applied science, Milwaukee, United States"	7	164
2	"Indian Institute of Management, Lucknow, India"	7	274
3	"School of Computer science and Engineering, Singapore city, Singapore"	7	258
4	"University of Oxford, United Kingdom"	7	253
5	"University of St. Gallen, Switzerland"	11	641

Source: Researchers' compilation

Table 6.2: Leading organizations as in May 2025

S. No.	Organization Name	No.of	Citations
1	"Department of Electrical Engineering and computer science,	4	79
2	"Department of mathematics, Illinois state University, United	3	70
3	"Department of law, economics, politics and modern languages,	3	16
4	"Department of Electrical and Computer Engineering, University of	2	63
5	"Chair of mathematical finance, technical university of Munich"	2	21

Source: Researchers' compilation

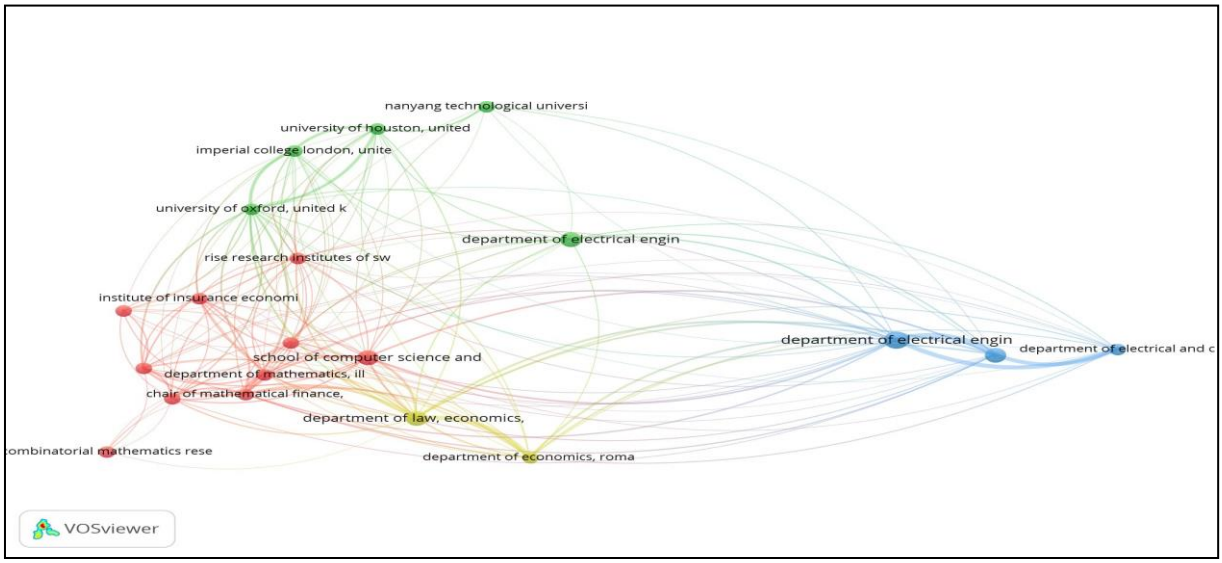

Figure 5: Leading organizations

Source: Researchers' compilation

The top organizations with maximum published work on CI as analysed by VOSviewer are illustrated in Table 6.1, 6.2 and Figure 5. Indian authors have been contributing more from the applied and empirical perspective, focusing on frameworks that combine AI-driven analytics and decision support with cyber-risk management. For instance, proposing a hybrid framework using explainable AI (XAI) for defence and recovery against phishing attacks, published in Decision Support Systems (Biswas et al., 2024). These contributions also highlight the growing role of modern information systems, which integrate intelligent analytics with organizational cyber-resilience strategies to enable real-time threat detection, adaptive decision-making, and improved incident response. Michigan leads in theoretical, model-based approaches and Indian researchers are carving a niche in AI-based, data-driven, and application-orientated frameworks for CI and cyber-risk management. Subsequent contributions, such as Embracing and controlling risk dependency in cyber-insurance policy underwriting, extend this perspective by exploring underwriting strategies in contexts where risks are highly correlated (Khalili et al., 2019).

3.1.5 Top Countries

This section presents leading countries based on the total number of publications identified in VOSviewer. USA leads the publication count on Cyber Insurance from 103 documents in May, 2025 (Table 7.2) to 109 documents in September, 2025 (Table 7.1). One of the most influential empirical studies in USA has examined the costs and causes of cyber incidents, highlighting that financial losses were often smaller than expected, which raised questions about firms' willingness to adopt CI (Romanosky et al., 2019). Another significant US contribution is by "Cremer", who has conducted a systematic review and highlighted the lack of standardized and accessible cyber-risk datasets, emphasizing on the data scarcity challenge in underwriting and pricing (Cremer et al., 2022).

Table 7.1: Top Countries ranked by number of documents as in September, 2025

S.No.	Country	No. of Documents	Citations
1	"United States"	109	2676
2	"United Kingdom"	40	575
3	"Germany"	21	457

4	"India"	17	337
5	"China"	17	132

Source: Researchers' compilation

Table 7.2: Top Countries ranked by number of documents as in May, 2025

S.No.	Country	No. of Documents	Citations
1	"United States"	103	2250
2	"United Kingdom"	32	460
3	"Germany"	21	358
4	"India"	17	282
5	"Switzerland"	9	439

Source: Researchers' compilation

India, although contributing fewer papers, has focused on application-driven and context- specific frameworks. Biswas proposed a hybrid framework using explainable AI (XAI) to defend against phishing attacks, linking AI innovations with cyber-risk mitigation (Biswas et al., 2024). Similarly, Sharma and Mukhopadhyay have contributed multiple frameworks for cyber-risk management, ranging from online gaming (Sharma & Mukhopadhyay, 2021) to smart city traffic systems (Sharma & Mukhopadhyay, 2022), reflecting the country's focus on practical and sectoral cyber-insurance challenges

Together, these streams of research highlight how the USA and UK dominate through empirical validation and modeling, while India is focusing on applied, AI-driven, and sector-specific approaches, thus diversifying the global discourse on CI.

Table 7.1,7.2 and Figure 6 shows that, USA and UK have marked their dominance. India maintained its document count with (n=17) while citations rose from 282 to 337. China also emerged as a co-leader with 17 documents. For India, the rising citation count reflects growing recognition, but China's entry indicates the need for India to sustain and expand its bibliometric footprint to remain competitive in the region.

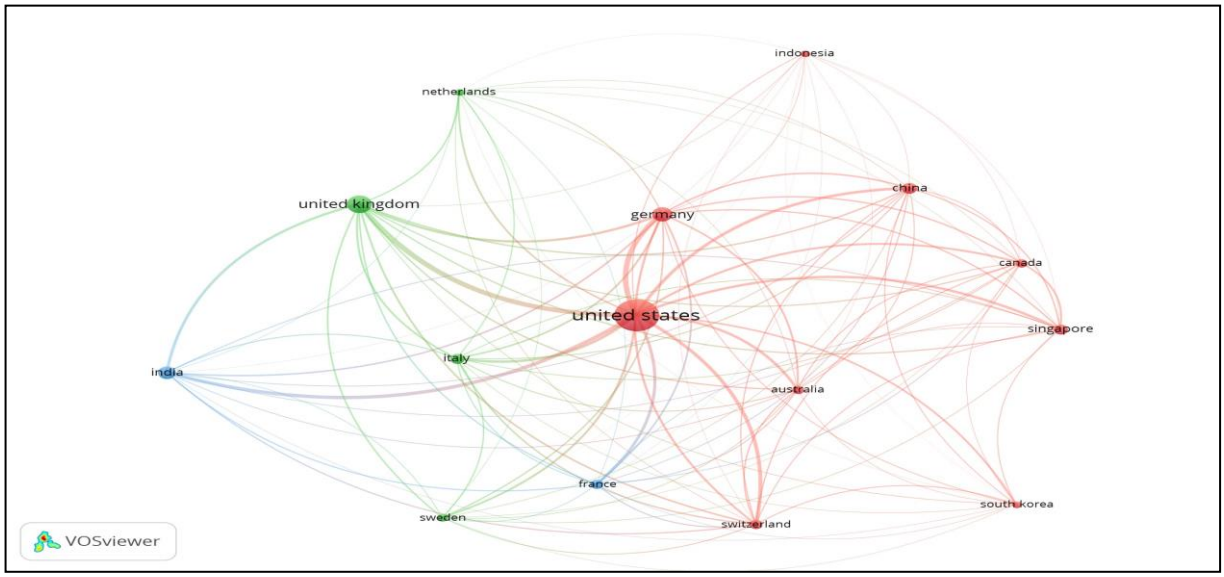

Figure 6: Top Countries

Source: Researchers' compilation

3.2 Co-authorship analysis

3.2.1 Leading authors

In this section co-authors with the highest productivity, as determined by their overall link strength, are shown. Table 8.1 and Figure 7 illustrates top authors by total link strength as in September, 2025. It also highlights additional authors e.g., Wei, W. and Liu, Z. entering the top ranks, with Niyato's citations increasing to 310 as compared to 275 (Table 8.2) which lists the top authors by total link strength as in May, 2025. This reflects the expanding author network in the

field of CI. Bibliometrically, this shows diversification of collaboration structures. For India, stronger co-authorship networks with these emerging authors could expand international reach, especially in AI-driven cyber risk modelling where India has already contributed.

Table 8.1: Top authors by total link strength as in September, 2025

S. No.	Author	No. of Documents	Citations	Total link strength
1	Wang L.	7	164	18
2	Wei,W.	7	164	18
3	Liu, Z.	6	153	16
4	Ten, chee	5	144	14
5	Niyato, D.	8	310	8

Source: Researchers' compilation

Table 8.2: Top authors by total link strength as in May, 2025

S. No.	Author	No. of Documents	Citations	Total link strength
1	Wang L.	7	152	18
2	Liu	6	141	16
3	Ten,chee	5	136	14
4	Niyato D.	8	275	7
5	Wang P.	7	262	7

Source: Researchers' compilation

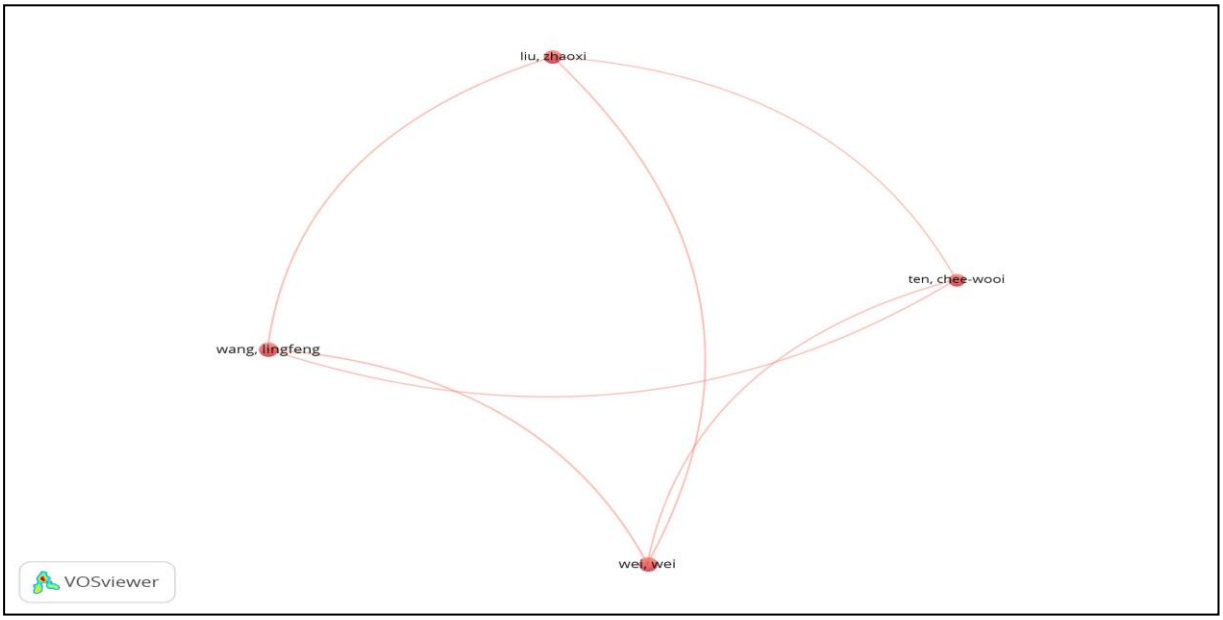

Figure 7: productive authors

Source: Researchers' compilation

3.2.2 Leading Organizations by Link Strength

Table 9.1, 9.2 and Figure 8 present the leading organizations determined by total link strength. Table 9.1 listing the top organizations by total link strength as in September, 2025 reflects the dominance of University of Oxford with seven documents and 253 citations. Bibliometric significance lies in the rising global connectivity of institutions with negligible contribution from Indian Organizations as illustrated in Figure 4. For India, the entry of IIM Lucknow underscores the need to leverage institutional collaboration strength and form stronger research partnerships with US and UK counterparts to amplify it's impact.

Table 9.1: Top organizations by total link strength as in September, 2025

S. No.	Organization	No. of Documents	Citations	Total link strength
1	"College of Engineering and applied science"	7	164	6
2	"University of Wisconsin-milwaukee"	6	153	6
3	"University of Kent, Canterbury"	6	79	1
4	"University of Oxford, United"	7	253	1
5	"Indian Institute of Management, Lucknow"	7	274	0

Source: Researchers' compilation

Table 9.2: Top organizations by total link strength as in May, 2025

S. No.	Organization	No. of Documents	Citations	Total link strength
1	"Department of Electrical Engineering and computer science, University of Michigan"	4	79	5
2	"Department of mathematical Science"	3	70	5
3	"Department of Electrical and Computer Engineering, University of Manitoba, Canada"	2	63	4
4	"University of Houston, United States"	2	42	3
5	"Imperial College London, United Kingdom"	2	139	2

Source: Researchers' compilation

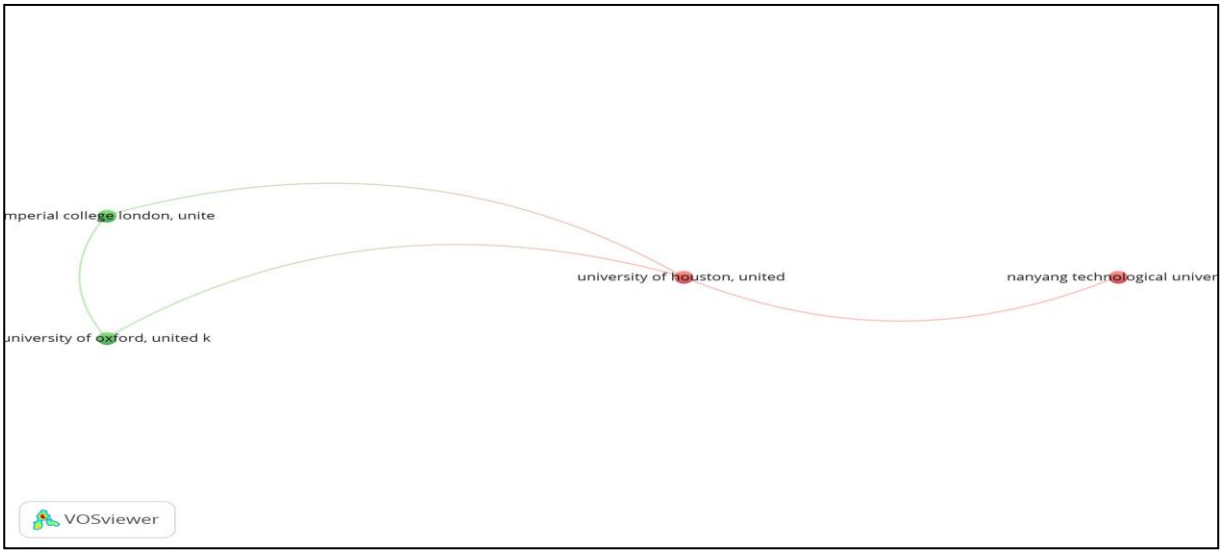

Figure 8: Top organizations

Source: Researchers' compilation

3.2.3 Top Countries by Link Strength

According to VOSviewer, results of top countries on the basis of co-authorship analysis are shown in Table 10.1, 10.2 and Figure 9. Table 10.2 lists top countries by total link strength as in May, 2025. The USA stands at first place with a total link strength of 49, with the "United Kingdom" and India following closely behind. Table 10.1 and Figure 5 illustrates the top countries by total link strength as in September, 2025 shows that "USA", "UK" and "India" have retained their leadership. India's citation count also increased from 282 to 337 while its link strength slightly dropped from 13 to 12 highlighting the need for cross country collaboration.

Table 10.1: Top countries by total link strength as of September, 2025

S. No.	Country	No. of Documents	Citations	Total link strength
1	"United States"	109	2676	32
2	"United Kingdom"	40	575	20
3	"India"	17	337	12
4	"China"	17	132	7
5	"Germany"	21	457	7

Source: Researchers' compilation

Table 10.2: Top countries by total link strength as of May, 2025

S. No.	Country	No. of Documents	Citations	Total link strength
1	"United States"	103	2250	49
2	"United Kingdom"	32	460	21
3	"India"	17	282	13
4	"Singapore"	11	316	10
5	"China"	13	109	9

Source: Researchers' compilation

Though, India's position remains strong, but is not expanding fast enough in collaboration networks. Strategically, Indian researchers should aim for deeper international collaborations to enhance both link strength and citation influence.

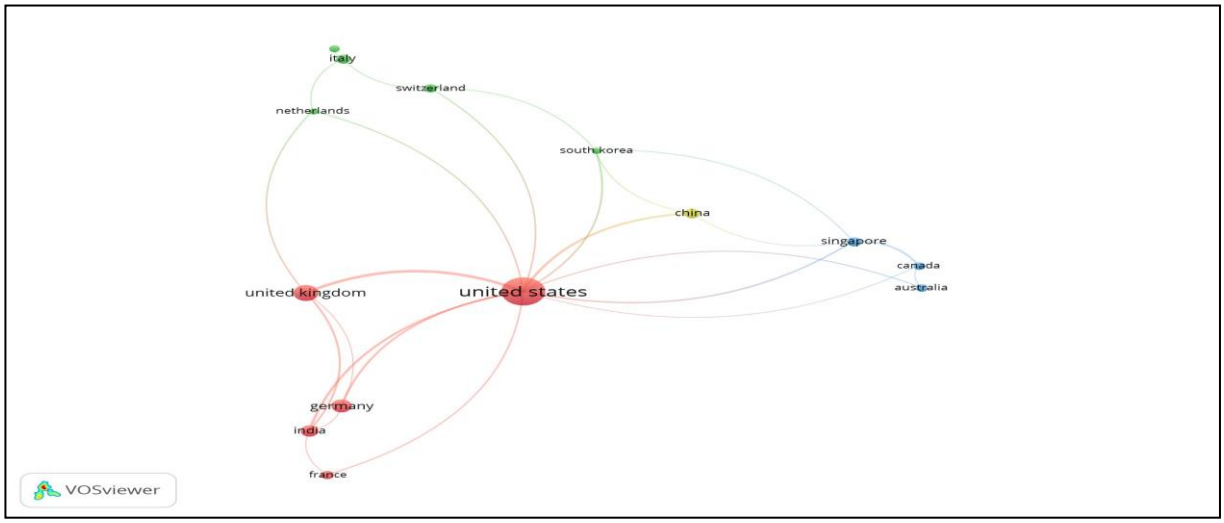

Figure 9: Top Countries

Source: Researchers' compilation

3.3 Co-citation analysis

It is done using cited authors, cited references, and cited sources. When two documents are quoted together in a third publication, the study finds whether they occur again or not (Nobanee et al., 2023). Researchers are able to identify the various trends of research topics in the field of study when two publications are co-cited (Nobanee et al., 2023).

3.3.1 Cited references

The findings of co-citation analysis of cited references as determined by VOSviewer are presented in Table 11.1, 11.2 and Figure 10.

Table 11.1: Cited references by total link strength as in September, 2025

S. No.	Cited Reference	Citations	Total link strength
1	"Biener, C.(2016)"	43	24
2	"Bandopadhyay. (2011)"	23	21
3	"Anderson,R. (2017)"	13	15
4	"Bessy-R. (2016)"	12	8
5	"Baer.W.(2016)"	11	7

Source: Researchers' compilation

Table 11.2: Cited references by total link strength as in May, 2025

S. No.	Cited Reference	Citations	Total link
1	"Eling and Schnell (2016)"	15	43
2	"Marotta et al. (2017)"	21	38
3	"Edwards et al. (2016)"	12	36
4	"Eling and Wirfs (2019)"	12	33
5	"Romanosky (2016)"	11	30

Source: Researchers' compilation

As shown in Table 11.2 published work of Eling and Schnell (2016) has a total link strength of 43 and is the top document as in May, 2025 followed by Marotta et al. (2017) and Edwards et al. (2016). Table 11.1 listing top cited references by total link strength as in September, 2025 shows the top cited references shift from Eling and Schnell (2016) to Biener (2015), with changes in total link strengths also.

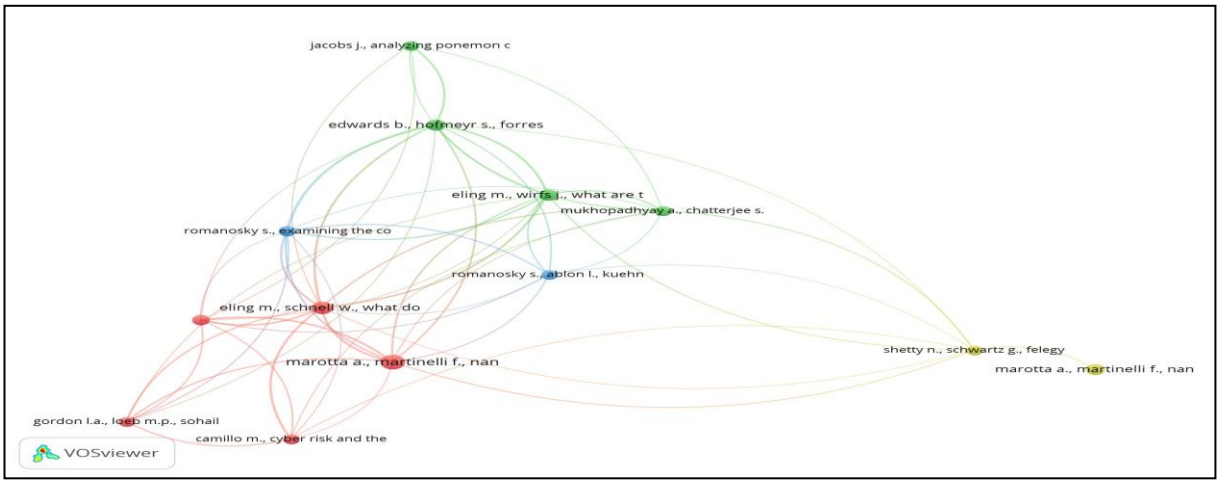

Figure 10: Cited references by authors

Source: Researchers' compilation

Overall there is a decrease in link strengths as new themes emerge, focus of research shifts. This is typical in fast moving fields such as CI. Importance lies in observing how intellectual structures evolve. While Eling and Schnell (2016) remain globally influential, the consistent reliance on Biener, C. and Bandhopadhyay shows that Indian studies are demonstrating integration with international reference structures.

3.3.2 Cited sources

Table 12.1 and Figure 11 lists the top cited journals according to the total link strength as in September, 2025. Computer and Security is the top most cited Journal with total link strength of 838, IEEE Access sands at second position with a link strength of 809, followed by Insurance: Mathematics and Economics, Journal of Cybersecurity and Risk Analysis.

Table 12.1: Cited sources by total link strength as in September, 2025

S. No.	Source	Citations	Total link strength
1	"Computer and Security"	80	838
2	"IEEE Access"	70	809
3	"Insurance: Mathematics and Economics"	64	765
4	"Journal of Cybersecurity"	79	728
5	"Risk Analysis"	61	676

Source: Researchers' compilation

Table 12.2: Cited sources by total link strength as in May, 2025

S. No.	Source	Citations	Total link strength
1	"Computer and Security"	80	838
2	"IEEE Access"	70	809
3	"Insurance: Mathematics and Economics"	64	765
4	"Journal of Cybersecurity"	79	728
5	"Risk Analysis"	61	676

Source: Researchers' compilation

There is no change in ranking or link strengths from May, 2025 to September, 2025 as shown in table 12.1 and 12.2. as compared to Table 12.2. It reflects stability in source indicating entrenched core journals. For India, this reinforces the strategy of targeting these core sources for both publishing and citing, thereby embedding Indian scholarship within dominant knowledge streams.

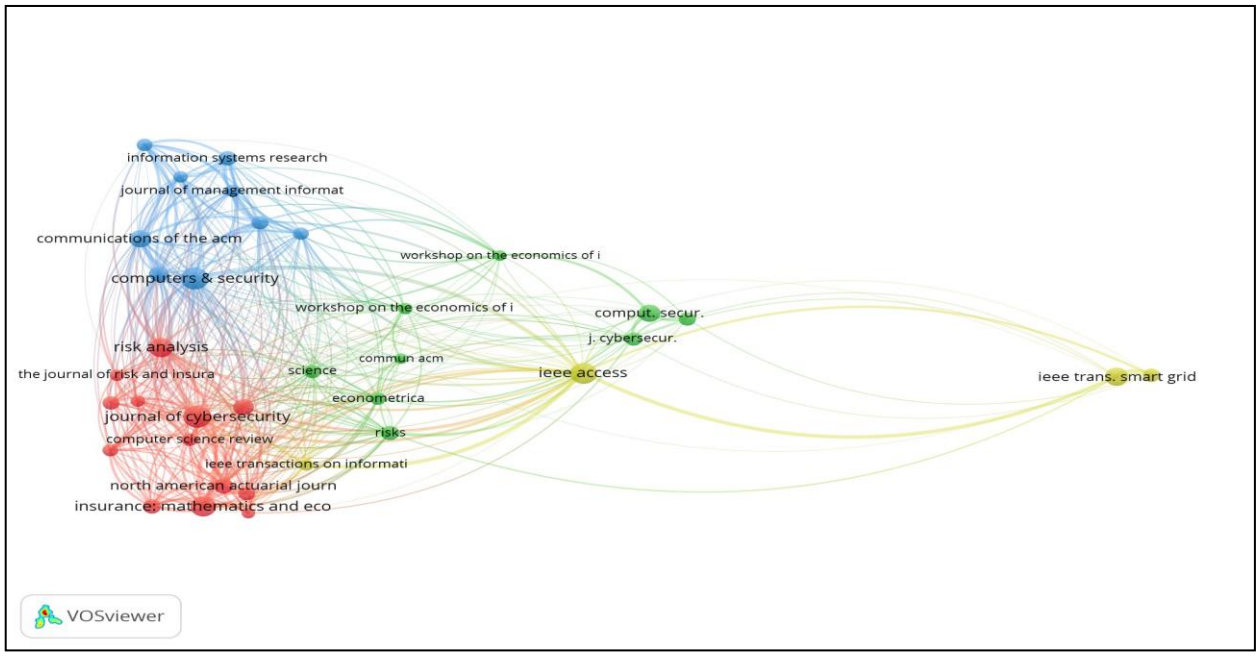

Figure 11: Top cited sources

Source: Researchers' compilation

3.4 Co-occurrence Analysis

Co-occurrence analysis is a bibliometric or text-analysis method used to identify how frequently two or more items—such as keywords, authors, concepts, or terms—appear together within the same documents. Figure 12 and 13 generated on Biblioshiny reveals a dominant research nexus between **'insurance'** (centered on risk assessment, economics,

financial markets) and **'cyber security'** focusing on cyber threats, risk management, cyber attacks, and computer crime as in September, 2025.

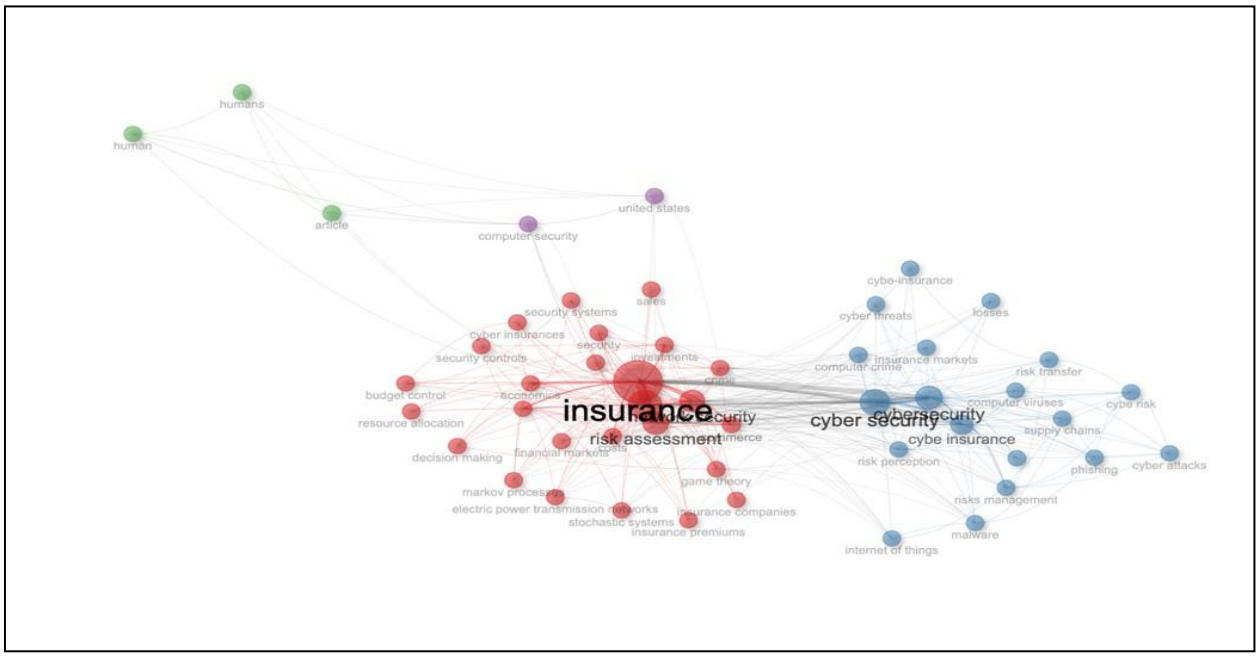

Figure 12: Co-occurrence Network

Source: Researchers' compilation

Figure 13: Word Cloud of Keywords

Source: Researchers' compilation

'Cyber insurance' has emerged as a critical bridging theme, linking these two major clusters. Secondary, less prominent clusters address foundational 'computer security' and the 'human' element in research. The overall landscape indicates a strong focus on managing and mitigating cyber risks through insurance mechanisms and risk assessment frameworks.

3.4.1 Prominent keywords by co-occurrence

The key terms highlighted in the research papers concerning cyber insurance as in May, 2025 are shown in Table 14.1. Every keyword helps in grasping main ideas within each search area. Commonly occurring keywords include "risk management", "insurance", and "cyber insurance". The keyword frequencies increased in the context of "Cyber Insurance" from 102 to 115 and "Insurance" from 83 to 95 from May, 2025 to September, 2025.

This reflects thematic intensification around CI. Keywords mirror the evolution of research priorities. For India, where CI is still a nascent concept, this trend validates the timeliness of focusing on cyber risk management and insurance adoption in the local research settings.

Table 14.1: Top keywords by co-occurrence as in September, 2025

S. No.	Keyword	Occurrence
1	"Cyber Insurance"	115
2	"Insurance"	95
3	"Cybersecurity"	66
4	"Risk Management"	60
5	"Cyber Security"	45

Source: Researchers' compilation

Table 14.2: Top keywords by co-occurrence as in May, 2025

S. No.	Keyword	Occurrence
1	"Cyber Insurance"	102
2	"Insurance"	83
3	"Risk Management"	53
4	"Cybersecurity"	64
5	"Cyber Security"	40

Source: Researchers' compilation

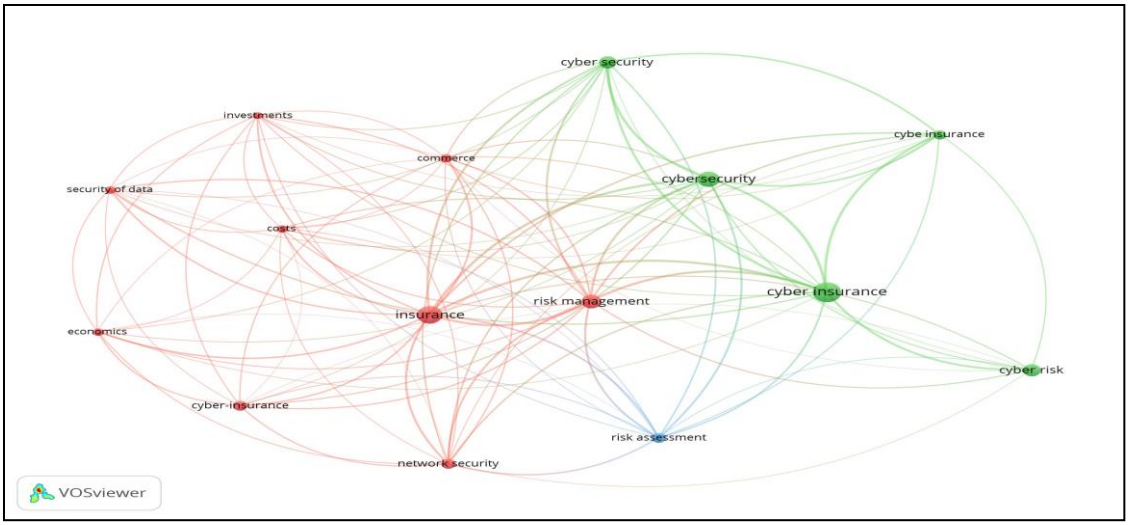

Figure 14: Top keywords

Source: Researchers' compilation

3.4.2 Top author keywords by co occurrence

The most three common author keywords based on co-occurrence as in May, 2025 include Cyber insurance, cyber risk, and Cybersecurity. Occurrences of keywords "Cyber Insurance" increased from 100 to 115, occurrence of "Risk Management" increased from 20 to 60 and occurrence of "Cybersecurity" increased from 41 to 66 as in September 2025.

Table 15.1: Top author keywords by co-occurrence as in September, 2025

S. No.	Keyword	Occurrence
1	"Cyber Insurance"	115
2	"Insurance"	95
3	"Cybersecurity"	66
4	"Risk Management"	60
5	"Cyber Security"	45

Source: Researchers' compilation

Table 15.2: Top author keywords by co-occurrence as in May, 2025

S. No.	Keyword	Occurrence
1	"Cyber Insurance"	100
2	"Cyber Risk"	42
3	"Cybersecurity"	41
4	"Cyber-Insurance"	26
5	"Risk Management"	20

Source: Researchers' compilation

This points on the fact that researchers increasingly tagging their work using the above mentioned keywords. It signals an expanding thematic network. For India, this validates the integration of global discourse with India's digital economy, where risk management frameworks are being actively explored in smart cities, finance, and governance contexts.

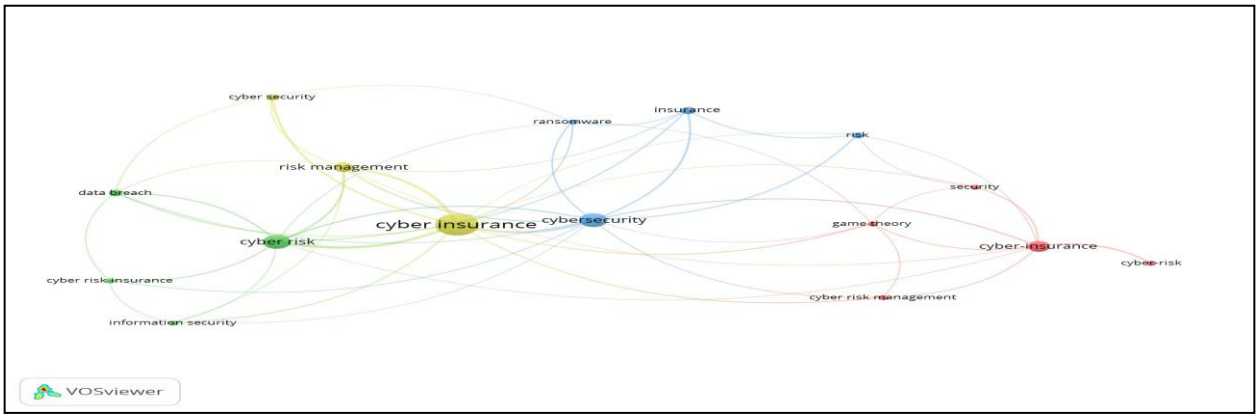

Figure 15: Top author keywords by co-occurrence

Source: Researchers' compilation

3.4.4. Index Keywords

This section highlights the most commonly used index terms. The top three index terms as in May, 2025 listed in Table 16.2 are cyber security, risk management, and insurance. The temporal analysis of word frequency as shown in Table 16.1, Figure 16 (extracted from VOSviewer) and Figure 17 (extracted from Biblioshiny) highlights the top index keywords as in September, 2025. It reveals 'Insurance' as a foundational key word with early and sustained growth, accelerating significantly post 2018. Figure 18 presents the word's frequency over time. More recently, 'Security of Data' has shown the most dramatic surge in cumulative occurrences, particularly since 2020, becoming a leading topic. Themes like 'Cybersecurity', 'Risk Management', 'Network Security', and notably 'Cyber Insurance' which have been emerging sharply after 2020 also demonstrate significant and accelerating growth.

This indicates a strong research shift towards these interconnected areas in the recent years, with 'Risk Assessment' and 'Economics' showing steadier, moderate growth, while 'Commerce' remains less prominent. These quantitative patterns of keyword co-occurrence and temporal trends point towards evolving research priorities. To understand the qualitative depth and nuances of these interconnected concepts, the study delves into the thematic analysis.

Table 16.1: Top index keywords by occurrence as of September, 2025

S. No.	Keyword	Occurrences
1	"Insurance"	80
2	"Risk Management"	45
3	"Cyber Security"	39
4	"Cybersecurity"	32
5	"Risk Assessment"	31

Source: Researchers' compilation

Table 16.2: Top index keywords by occurrence as of May, 2025

S. No.	Keyword	Occurrences
1	"Insurance"	72
2	"Risk Management"	40
3	"Cyber Security"	35
4	"Cybersecurity"	30
5	"Risk Assessment"	27

Source: Researchers' compilation

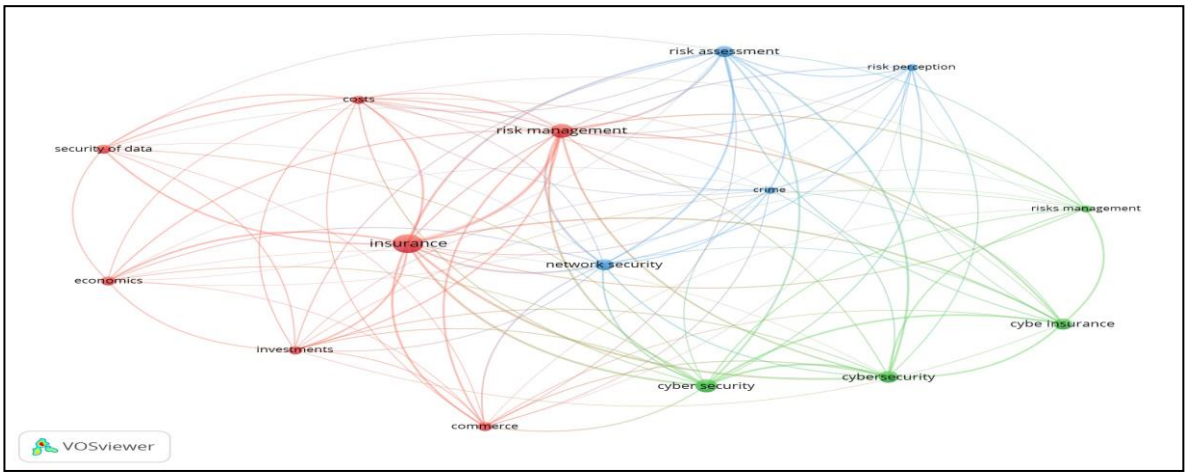

Figure 16: Top index keywords

Source: Researchers' compilation

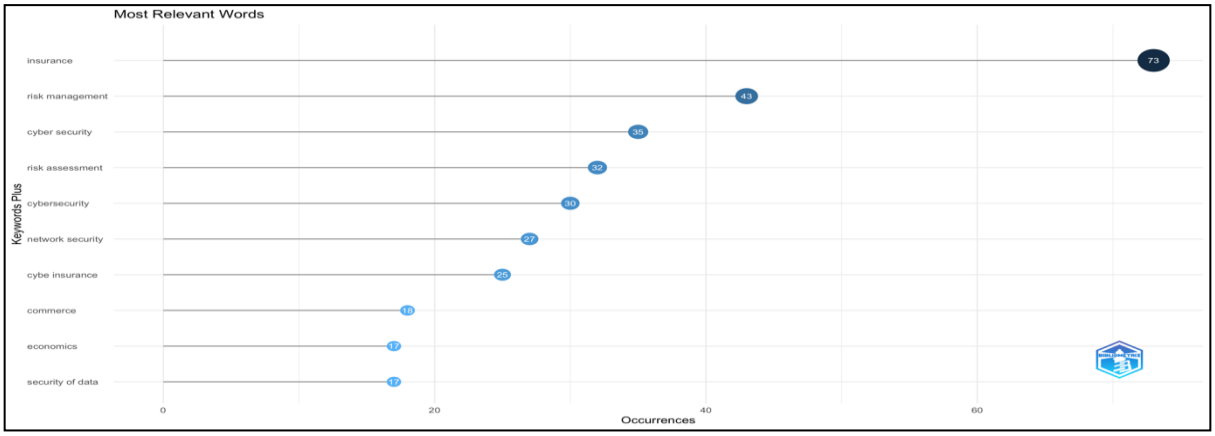

Figure 17: Most relevant words

Source: Researchers' compilation

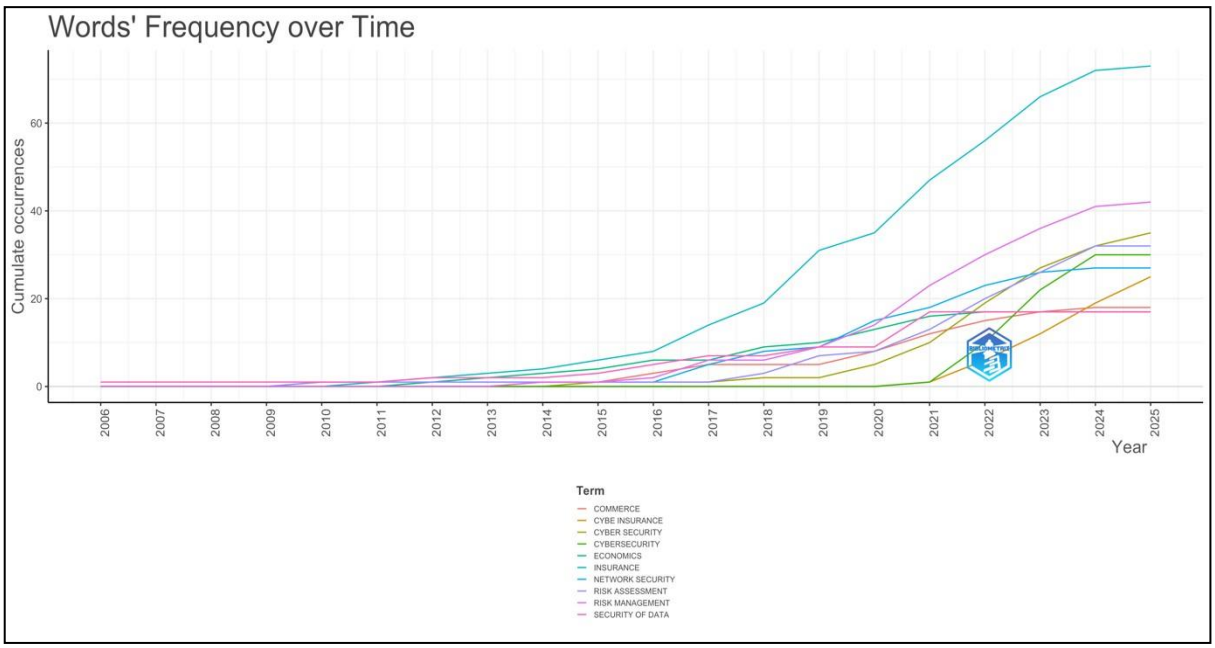

Figure 18: Word's Frequency Over Time

Source: Researchers' compilation

Table 16.1 highlights the top index keywords by occurrences as in September, 2025. It shows occurrences of "Insurance" rising from 72 to 80, "Risk Management" from 40 to 45, and "Risk Assessment" from 27 to 31. This points to consolidation of conceptual anchors in the field. It shows how stable yet expanding keywords define the intellectual core of a subject.

The comparative tables (2.1–16.1 vs. 2.2–16.2) demonstrate that even over a short temporal window of four months from May, 2025 to September, 2025, citation counts, author influence, organizational strength, and keyword usage have evolved significantly. This highlights the dynamic and cumulative nature of research visibility.

3.5 Thematic Analysis

Using Biblioshiny, Figure 19 presents a thematic map generating the themes surrounfing CI os presented in Figure 19. The following four major themes: "Motor Themes, Basic Themes, Niche Themes and Emerging/Declining Themes based on their development (density) and relevance (centrality)" have been identified.

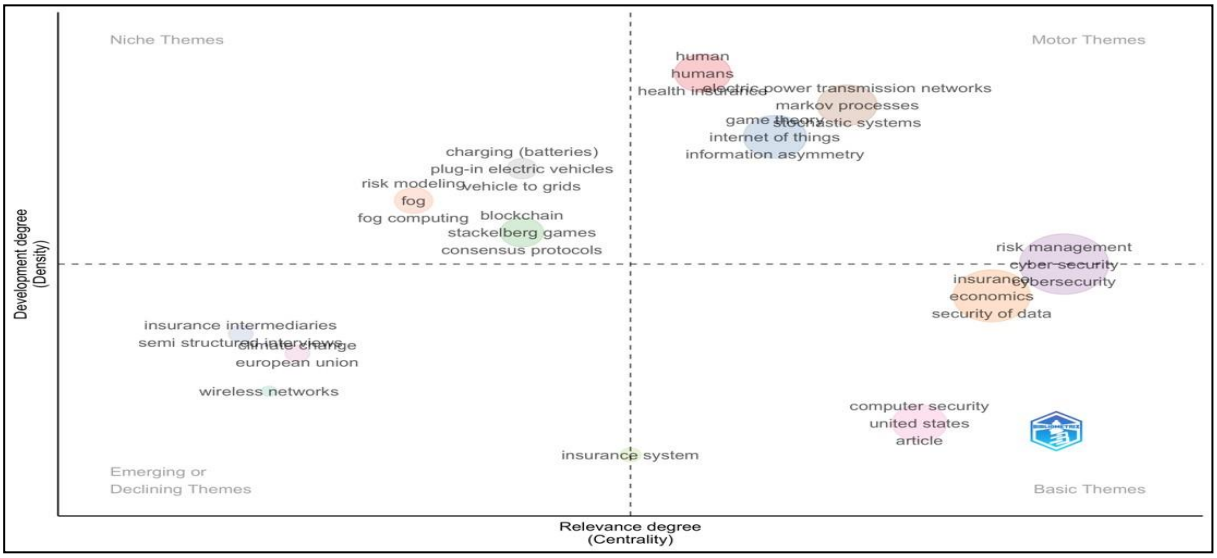

Figure19: Thematic Map

Source: Researchers' compilation

♦ **Motor Themes**: These themes are highly developed, central and they drive the core research agenda. For the present study, the themes identified span the upper right quadrant. These include **'Risk management/cyber-security'** and **'insurance/economics/security ofdata'.**

♦ **Basic Themes:** These include the foundational concepts like '**computer security'** and **'Insurance system'** that underpin the area with high relevance but lower internal development. In the present study these themes span the lower right quadrant.

♦ **Niche Themes:** They represent focused research areas that are well-developed internally but less central. Specialized topics such as **'risk modelling'** and **'blockchain'** are, representing such research areas. These themes span the upper left quadrant.

♦ **Emerging/Declining Themes:** It includes marginal themes indicating nascent or waning research areas. The theme **'insurance intermediaries'** is spanning the lower left quadrant is a part of this theme.

The relevance of thematic analysis lies in its ability to strategically map the intellectual structure of research domain. By identifying the well-established motor themes, foundational concepts, specialized niches, and areas of potential future growth or decline, it offers valuable insights for researchers seeking to position their work, practitioners aiming to understand key trends, and policymakers focusing on impactful areas within the evolving landscape of insurance and cybersecurity. This understanding helps direct future research efforts towards impactful or underexplored areas of Cyber Insurance.

3.6 Factorial Analysis

Factorial analysis, especially "Multiple Correspondence Analysis" (MCA), is a multivariate statistical method used to reduce the dimensionality of complex data and uncover underlying patterns or "conceptual dimensions" within a set of categorical variables (in this case keywords) (Varese & Zeng, 2024). It is used to create a "Conceptual Structure Map" from keywords.

The dendrogram shown in Figure 20 extracted from Biblioshiny illustrates a fundamental bifurcation in the research landscape as revealed by the hierarchical clustering. A distinct hierarchical structure may be seen in the dendrogram. It presents a hierarchial structure of keywords.

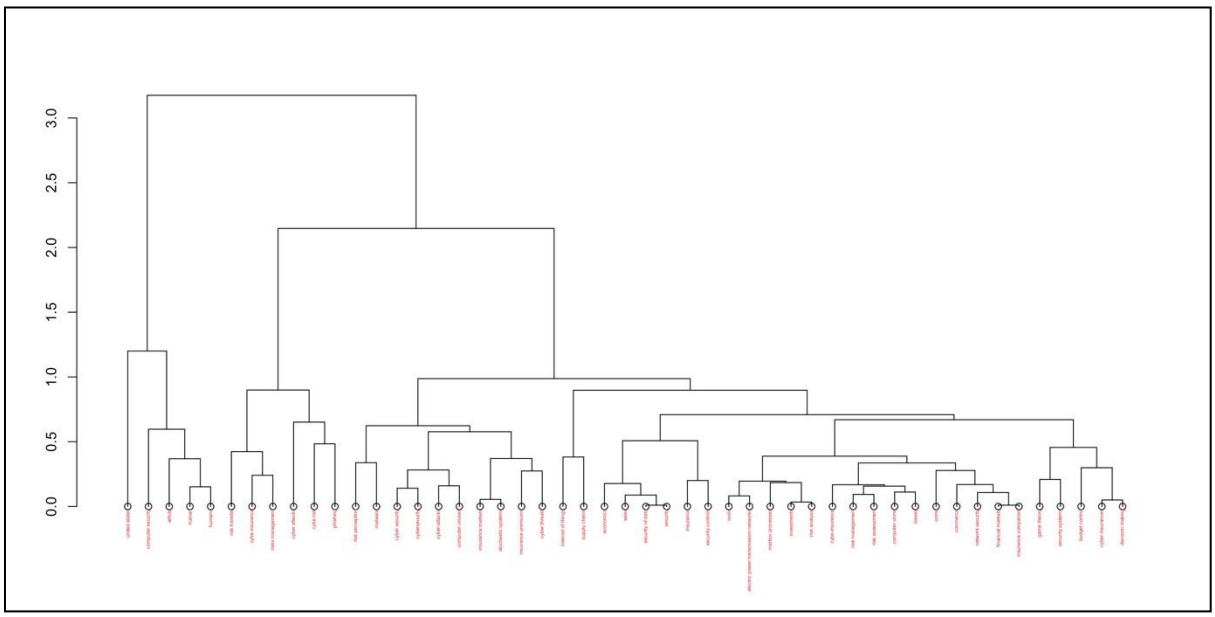

Figure 20: Dendogram

Source: Researchers' compilation

A fundamental divide distinguishes the key domain subjects from broader research context phrases such as "united states," "computer security," "human," and "article". Different clusters appear within the domain. One significant cluster such as "cybersecurity," "risk management," "cyberattacks," "phishing," "cyber insurance," and "risk perception" focuses on cybersecurity risks and mitigation. Terms such as "insurance," "economics," "security of data," "security controls," "insurance premiums," "budget control," "security systems," "losses," and "cyber crime" are examples of terms that fall under another cluster that focusses on the financial, operational, and institutional elements of insurance and security.

The Conceptual Structure Map produced by MCA as shown in Figure 21 comprehends the conceptual connections between these identified theme clusters and the dimensions along which they differ (Hernández-Lozada et al., 2025) .

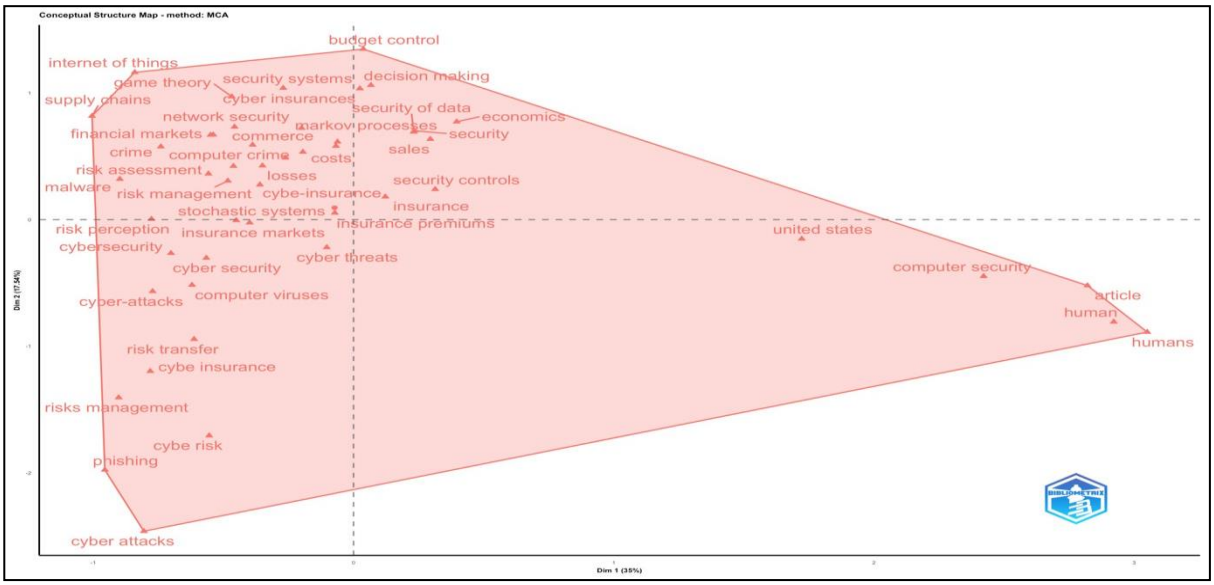

Figure 21: Factorial Map

Source: Researchers' compilation

MCA visually maps the conceptual relationships. Dimension 1 (accounting for 25% of the variance) clearly segregates the general research context terms e.g., 'human,' 'united states' to the right, from the dense core of domain-specific terms on the left and centre. Dimension 2 (17.94% variance) further differentiates within this core domain.

The upper portion highlights themes related to broader operational, economic, and systemic aspects such as 'budget control,' 'security systems,' 'decision making,' and 'economics'. The lower portion emphasizes more direct 'cyber threats' like 'cyber-attacks,' 'phishing', specific 'risk' types 'cyber risk', and 'risk transfer' mechanisms. Thematic analyses reveal that research clusters frequently revolve around the practical application of CI for businesses and its function in risk management, highlighting its perceived necessity in the contemporary economic landscape (Nobanee et al., 2023).

Notably, 'cyber insurance' and 'insurance markets' bridge these distinctions, appearing centrally, reinforcing their role as key linking concepts between broader insurance frameworks and specific cybersecurity challenges.

3.7 Cluster Analysis

A set of statistical methods and algorithms for classifying objects so that, if two items are in the same group, their association is maximal; if not, it is minimal is known as cluster analysis, or clustering. Large amounts of data may be efficiently categorised into a limited number of significant categories using cluster analysis (Nobanee et al., 2023).

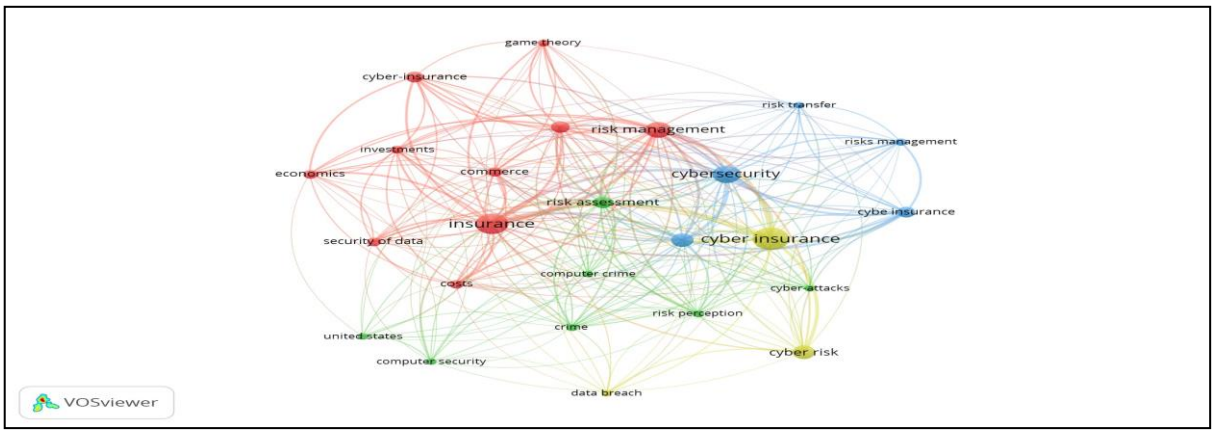

Figure 22: Co-occurrence of Keywords

Source: Researchers' compilation

Figure 22 extracted from VOSviewer presents the co-occurrence of keywords and identifies the clusters. It reveals distinct clusters of research themes, including "cyber insurance and cyber risk", "cyber insurance and businesses", "cyber insurance and technology", "cyber insurance contracts and information sharing", and "cyberattacks and security controls" (Nobanee et al., 2023a).

The identified thematic clusters further supports the publication trend, with significant groupings of research around "cyber insurance and businesses" and "cyber insurance and risk management". These clusters highlight that the academic community is actively exploring how Cyber Insurance supports business continuity, resilience, and the overall management of cyber- related financial exposures (Nobanee et al., 2023).

Four clusters have been identified for the present work on Cyber Insurance as shown in Figure 22

Cluster 1: Commerce, costs, cyber insurance, economics, game theory, insurance, investments, network security, risk management, security of data, game theory

Cluster 2: Computer crime, computer security, crime, cyber-attacks, risk assessments, risk perception, United States.

Cluster 3: Cyber Insurance, cyber security, cybersecurity

Cluster 4: Cyber Insurance, Cyber Risk, data breach

These clusters appear in different colours can be compared with the themes generated with the help of Biblioshiny. These groups greatly align with the clusters identified in the dendrogram as well as the motor and niche themes from the thematic map as presented in Figure 19 and 20. However there are a few words grouped differently like .., this might be due to the different algorithms.

4. Conclusion

The present work provides a comprehensive interpretation of the literature on the CI detailed insight using Biblioshiny and VOSViewer about the literature on Cyber Insurance. Due to the vital importance of cybersecurity concerns and the growing threat of cyberattacks, a detailed analysis is imperative. Key findings have been uncovered by the study through factorial analysis (Multiple Correspondence Analysis), temporal trend analysis, thematic mapping, and keyword co-occurrence mapping, using unique clustering algorithms and potent network visualisation features. Findings refer a majority of citations by Biener et al. (2015) and Mukhopadhyay (2013) highlight integration of global literature to India-specific research on risk modelling and cybercrime legislation, reflecting India's growing contribution to the global discourse. The analysis consistently identified a dominant research nexus between foundational 'insurance' principles (risk assessment, economics) and pressing 'cybersecurity' challenges (threats, risk management), with 'cyber insurance' acting as a central, bridging theme. From the thematic patterns some secondary but meaningful clusters have been captured that include 'computer security' foundations and the 'human' element of cybersecurity, thereby reaffirming that cyber insurance functions as a crucial link across these domains. "Risk management/cyber-security" and "insurance/economics/security of data" are the two major areas guiding contemporary study. Research on "security of data," "cybersecurity," "risk management," and "cyber insurance" itself has notably increased in recent years.

This growth is further reflected in author-keyword dynamics captured from May 2025 to September 2025. This shows rise in occurrences among the keywords "Cyber Insurance", "Risk Management", and "Cybersecurity". Thus indicating that researchers are increasingly tagging their work with these core concepts and expanding the thematic network an especially relevant trend for India, where such terminology aligns with research in smart cities, financial technologies, and digital-governance ecosystems. These theme categories and their linkages have been graphically emphasised by the thematic map developed. The tools used discovered intellectual structure, providing varied clustering perspective and highly interactive network visualisations that clearly define thematic communities, and offered detailed quantitative data trends, hierarchical structures (dendrograms), and strategic thematic diagrams (density/centrality maps). This dual approach increased the validity of the discovered intellectual structure. With no changes in ranking among journals publishing work on CI and no changes in link strengths between May 2025 and September 2025 signals a stable set of entrenched core journals. This provides a clear roadmap for targeting these sources to embed intellect on CI in Indian context within globally dominant knowledge streams. The results highlight the importance of Cyber Insurance and its increasing relevance, thus, confirming the need for enhanced research. The themes and structures like 'Risk management/cyber-security', 'computer security', 'Insurance system', 'risk modelling', 'blockchain' and 'insurance intermediaries' found through analysis provide a taxonomy that would help Government, lawmakers, practitioners, and insurance firms etc. to build policies, create rules and comprehend coverage.

The study highlights a significant and growing body of literature demonstrating the increasing academic and industry interest in the domain, particularly from 2009 onwards (Schutz et al., 2023). The study identified key thematic clusters, including the intersection of Cyber Insurance with businesses, technology, contracts, and the broader topic of cyberattacks and security controls (Schutz et al., 2023). The extensive citation of key papers and the identification of productive authors in this domain also point to the deepening engagement and recognized importance of Cyber

Insurance within the academic discourse. The study recognized influential authors and publications that have shaped the discourse in this field, alongside the prominent journals and institutions contributing to its advancement. The increasing research output signifies the evolving recognition of "Cyber Insurance" as a crucial component of modern risk management strategies in the face of escalating cyber threats. In the Indian context, these scholarly trends harmonise with the broader shift toward integrating cyber-risk assessment and insurance frameworks into its fast-digitising economy, reinforcing India's alignment with the global Cyber Insurance research landscape.

5. Limitations

The analysis focuses on keywords and metadata, which could not adequately convey the nuances or hidden information found in the published work. Bibliometric analysis is useful for mapping trends and structures, but it is not enough on its own to completely comprehend the qualitative depth or real-world applications of Cyber Insuance solutions. It only identifies patterns and skips over the nuances of policy wording or the efficacy of particular risk mitigation techniques described in individual papers. While bibliometric analysis reveal the trends and influential works, it does not delve into the qualitative content of the research, thus limiting a deeper understanding of the nuances within specific studies (Schutz et al., 2023b).

4months

6. Future Research

Looking ahead, several avenues for future research emerge from this analysis. Further bibliometric studies could expand the scope by including additional databases and employing a broader range of keywords to capture a more exhaustive body of literature. A qualitative review of the identified key papers would offer deeper insights into the specific findings and methodologies employed in influential CI research. Moreover, future work could explore the geographical distribution of research and collaborations, as well as investigate the impact of CI on market development and regulatory frameworks (Nobanee et al., 2023a).

There are various future avenues for research such as investigating Niche and Emerging Themes. Many such themes have been identified in the thematic mapping such as blockchain, game theory, emerging or declining themes e.g. climate change in relation to cyber risk. Complementary qualitative research such as Systematic Literature Reviews can also be performed focusing on the highly cited papers within the identified clusters. Given the dynamic nature of cyber threats and insurance products, longitudinal studies tracking the evolution of CI research themes and their practical implications would also be highly valuable. Further the interdisciplinary connections can also be explored for example, the role of 'human' identified as a cluster opens the avenues of studying human behaviour in context of CI. Future researchers can also explore the impact of technology on CI. To sum up, this work offers a thorough summary of the current landscape of research on Cyber Insurance, emphasising its components, development, and main areas of focus.