The Cognitive Cartography of Cybersecurity: India's Knowledge Pathways and Scholarly Networks

Kishore Dey*

Librarian, Karunamoyee Library, Government Sponsored Public Library, Kolkata, West Bengal, INDIA.

ABSTRACT

Purpose/Background: This research employs a bibliometric study to understand the Indian scenario of cybersecurity research from 2016 to 2025. The paper deeply examines the research, and the research and development are the key focuses. **Methodology:** The article has been based on an OpenAlex database inquiry, analysis by R (Bibliometrix/Biblioshiny), and Microsoft Excel. The investigation examined 3,374 Indian documents. **Results:** The examination of 3,374 Indian documents has resulted in the finding of an extraordinary annual growth rate of 58.57% which was facilitate by the equally strong international collaboration trend and the dominance of journal articles and book chapters. SRM Institute of Science and Technology, Chitkara University, and Lovely Professional University were identified as top productive affiliations. The prominent keywords such as computer science, artificial intelligence, internet privacy, and machine learning indicate the technological and ethical side of the cybersecurity research in India, which are merging. **Conclusion:** In essence, the discoveries delineate India's intellectual and collaborative frameworks that mirror an at-depth-interdisciplinary knowledge ecosystem, which is growing and thus in line with the global digital security priorities.

Keywords: Artificial Intelligence, Bibliometrics, Cybersecurity, India, Knowledge Mapping, OpenAlex, Scholarly Collaboration.

Correspondence:
Mr. Kishore Dey
Librarian, Karunamoyee Library,
Government Sponsored Public Library,
Kolkata, West Bengal, INDIA.
Email: kishore.ju29@gmail.com

Received: 12-08-2025;
Revised: 02-09-2025;
Accepted: 24-11-2025.

INTRODUCTION

Cybersecurity has become an essential tool for maintaining the integrity, confidentiality, and availability of data and information systems in all sectors in the digitally fast-moving major era. Cybersecurity threats and vulnerabilities of the digital infrastructure rise with the increase in technological advances; thus, cyber security investigation is a top global priority. Research indicates that the domain has transitioned from only using technical models to multidisciplinary topics, such as artificial intelligence, sustainable development, behavioural sciences, and data ethics (Sulich *et al*., 2023; Zainal *et al*., 2025). Additionally, the rise of research on cybersecurity and artificial intelligence is the ultimate proof of their mutual dependence in the creation of advanced defence mechanisms and predictive systems (Albahri and Alamoodi 2023; Purnama *et al*., 2024).

India with its digital economy, which is growing rapidly, and the implementation of the National Cyber Security Policy and Digital India, has been benefited from a remarkable increase in research related to cybersecurity. Present scientometric and bibliometric studies have shown that India is a major player in global cybersecurity scholarship through collaborations internationally and research done by AI-driven directions (Loan *et al*., 2022; Elango *et al*., 2023). Nevertheless, current research has mostly concentrated on worldwide trends, applications to healthcare, or particular technological areas like IoT and machine learning (Jalali *et al*., 2019; Ganji and Afshan 2025; Coman *et al*., 2025), whereas detailed country-specific mapping of Indias cognitive and collaborative structures is scarcely available.

The focal point of this study is to close the gap in the research by profiling the scholarly Indian cybersecurity landscape from 2016-2025 utilizing OpenAlex database supplied data. The research through R (Bibliometrix/Biblioshiny) and Microsoft Excel visualizes the trends in publications, major authors, sources for referenced works, essential institutional affiliations, and the most frequently used keywords. This paper through the assemblage of a cognitive map of the Indian research in cybersecurity, extends, in effect, a systematic survey of, among other aspects, the topics and sub-topics covered, the research developmental stages, and the academic linkages, thus presenting an empirically-grounded understanding of Indias dynamic stance in the global cybersecurity research ecosystem.

DOI: 10.5530/irc.2.3.34

Publishing Partner : Manuscript Technomedia. [www.mstechnomedia.com]

LITERATURE REVIEW

The extensive development of digital infrastructure and the increasing number of cyber-attacks have made cybersecurity research an essential area of concern for a global academic and policy. Many bibliometric and scientometric studies have examined its evolving patterns, collaboration networks, and thematic trends. To identify the emerging areas of cybersecurity and data protection, (Coman *et al.*, 2025) performed a bibliometric and semantic analysis of publications from the Web of Science, which indicated numerous innovative-direction changes led by dynamic innovation. In the same way, (Abidin *et al.*, 2025) performed a study on cybersecurity behaviour using Scopus data, thereby demonstrating steady growth of publications and that the United States, and China research has been the most influential, while advanced bibliometric tools such as VOSviewer and Publish or Perish were used for the analysis.

Being at the crossroad between technology and eco-friendliness, (Sulich *et al.*, 2023) explored the interconnection between cybersecurity and sustainable development, and pointed out the urgency of establishing security frameworks that are in line with the global sustainability goals. Using Biblioshiny and VOSviewer, Ganji and Afshan (2025) carried out a detailed study on the IoT security, the authors uncover AI-driven and blockchain-enabled ethical innovations (Nobanee *et al.*, 2023). Pinpointed the primary contributors and the gaps for the cybercrime research area, whereas Albahri and Alamoodi (2023) predicted rapid changes in AI-powered cybersecurity research with deep learning, IoT, network defence as the major areas of application.

On a local scale, (Loan *et al.*, 2022) documented a massive increase in publication and high level of international cooperation with India being one of the major contributors. (Jalali *et al.*, 2019) drew attention to the lack of healthcare cybersecurity research, whereas (Purnama *et al.*, 2024) illustrated how machine learning could revolutionize cyber defence. One can add that (Elango *et al.*, 2023) pinpointed India to be a major source with highly interactive co-authorship networks and a growing focus on AI and cloud computing. The overall narrative these documents provide is that the field of cybersecurity is evolving into an extensively interdisciplinary one in which the integration of AI, IoT, sustainability, and behavioural science is happening, and that it is heading towards the use of data-driven security paradigms that are morally aware.

OBJECTIVES OF THE STUDY

The essential objective of this research is to understand the changing and diversified intellectual trends in cybersecurity research in India by conducting a detailed and scholarly output review. After thoroughly collecting the data from OpenAlex and performing the analysis with R (Bibliometrix/Biblioshiny) and MS Excel, the study is set to attain the following goals:

I. To examine the annual publication trend of cybersecurity research in India between 2016 and 2025,

II. To identify the most prolific authors contributing to cybersecurity research,

III. To analyze the top publication sources, including journals, books, and conference proceedings,

IV. To explore institutional affiliations and to investigate the most frequently used keywords within cybersecurity discourse in India.

METHODOLOGY

Current research utilizes an interpretive quantitative method to study the cognitive structure and the scholarly dynamics of Indian cybersecurity research literature. The OpenAlex database, which provides full and open metadata for global scientific output, was the source of the bibliographic data. The data extraction was done on 10 November 2025 with the search query "cybersecurity" in the title and abstract fields and has brought about 63,270 records worldwide. In order to establish a contextual focus, the first filters of the results were applied to the country (India, 3,443 records), year (2016-2025, 3,431 records), and language (English, 3,374 records) consecutively. The last dataset was saved locally in CSV format and was pre-processed in Microsoft Excel to standardize author names, keywords, affiliations, and source titles, as well as to remove incomplete or duplicate entries.

The sanitized data were subjected to analysis with R and RStudio through the Bibliometrix and Biblioshiny packages for revealing the intellectual contours of Indian cybersecurity research. The outputs were visualized and refined by Microsoft Excel for generating interpretive diagrams and tables that, when merged, exemplify India's knowledge pathways and scholarly networks in cybersecurity from a cognitive cartographic perspective.

ETHICAL STATEMENT

This study is based entirely on secondary bibliographic data obtained from the OpenAlex open-access database. No human participants, confidential information, or personally identifiable data were involved. Therefore, ethical approval was not required. All data used are publicly accessible, and due care was taken to ensure accuracy, transparency, and responsible research practices.

DATA ANALYSIS AND FINDINGS

The research scene based on the OpenAlex dataset has pretty much been lively and changing rapidly in the area of India cybersecurity from 2016 to 2025. After country, language, and year filtering the data, there were found to be 3,374 Indian research contributions out of 63,270 publications on cybersecurity worldwide. A very strong indication of the output of research has been increasing at a very rapid speed over time is the annual growth rate of

58.57%. The predominance of journal articles (66.4%) indicates a strong commitment to peer-reviewed dissemination, whereas the considerable share of book chapters (24.8%) discloses India's participation in the collaboration of edited works. The average citations per doc of 7.93 with the average document age of fewer than two years is a strong indication that the field is very active and quite recent and is attracting more and more scholarly circles (see Table 1).

The average authorship pattern of 3.58 authors per paper and 24.21% of international collaboration of India cybersecurity research are very clear indications that India cybersecurity research is a networked and interdisciplinary approach. Such a collaboration has the potential to deepen the scholarly engagement and expose Indian scholars to more global cybersecurity discourses. The continued increase of multi-authored papers is also a sign of the Indian scholars' departure from the traditional method of individual authoring to a collective approach of knowledge production, which is a typical international research practice. In fact, the findings portray India cybersecurity scholarship as a lively, cooperative, and rapidly expanding one with a large capacity to influence the policy and generate new technology.

Publication Trend by Year

The trajectory of the publication of cybersecurity research in India over the period 2016-2025 reveals a phenomenal growth trend, which accelerates with time. The number of articles was barely 10 in 2016 and 9 in 2017, so the output of research was minimal during these years and only in 2018 did it start to grow steadily. The number of publications grew to 59 in 2019 and nearly doubled to 124 in 2020, thus marking the beginning of a regular upward trend. After the pandemic, there was a very sharp increase in the number of publications, which went from 245 in 2021 to 414 in 2022, and then there was a huge jump to 753 in 2023. The year 2024 was the most fruitful with a total of 1095 publications and the productivity not only mirrored internal institutional prioritization but also wider academic engagement with cybersecurity themes. The year 2025 is still trending with a slight decrease of 634 publications (year's data is still ongoing), but the total direction of the growth curve is showing an average annual growth rate of 58.57% which is indicative of the country's increasing attention to digital security, data protection, and technological sovereignty through scholarly research (see Figure 1).

Leading Contributors to Cybersecurity Research in India

An authorship examination reveals that Chinnaraji Annamalai with 39 publications is the one who mostly initiated cybersecurity research in India and as a result, is the dominant individual contributor. After him, Akashdeep Bhardwaj and Ishu Sharma with 24 and 19 articles, respectively, may be traced for their active and lengthy contributions. The number of papers of each of the four writers Brij B. Gupta, C. V. Suresh Babu, Keshav Kaushik, and Mohit Tiwari implicate a potentially strong collaborative engagement, thus, they are the group of a few scholars. Moreover, the authors Bhupinder Singh, Aadil Khan, and Atul Kumar are quite respective in the research field, each with more than 10 papers (see Table 2). The difference between the total and fractionalized counts discloses the collaborative nature of Indian cybersecurity research, which is a field where co-authorship is the main way to progress.

Leading Publication Sources in Cybersecurity Research

Analyzing the locations of the publications reveals that publications in book series and open-access platforms have been the prominent means of spreading cybersecurity research from India. The two book series "Advances in Computational Intelligence and Robotics" and "Advances in Information Security, Privacy, and Ethics" jointly account for nearly 18% of the total

Table 1: Overview of Cybersecurity Research in India (2016-2025).

Indicator	Description	Value
Database	Source of data extraction	OpenAlex
Extraction Date	Data collected on	10 November 2025
Total Publications	Number of Indian documents (2016-2025)	3,374
Total Sources	Distinct journals, conferences, and books	733
Total Authors	Contributors involved in the dataset	9,582
Authors per Document	Collaboration intensity	3.58
International Co-authorship (%)	Cross-border collaboration rate	24.21%
Annual Growth Rate	Publication growth per year	58.57%
Average Citations per Document	Citation impact indicator	7.93
Document Types	Articles (66.4%), Chapters (24.8%), Reviews and Others (8.8%)	-
Average Document Age	Mean publication recency	1.83 years
Analysis Tools	Software used	R, RStudio (Bibliometrix/ Biblioshiny), Excel

Table 2: Top Ten Prolific Authors.

Rank	Author	Articles	Articles Fractionalized
1	Chinnaraji Annamalai	39	39.00
2	Akashdeep Bhardwaj	24	16.73
3	Ishu Sharma	19	9.03
4	Brij B. Gupta	15	3.24
5	C. V. Suresh Babu	15	4.83
6	Keshav Kaushik	15	7.43
7	Mohit Tiwari	15	2.51
8	Bhupinder Singh	13	5.15
9	Aadil Khan	12	5.34
10	Atul Kumar	11	4.92

publications, thus indicating a strong inclination towards edited academic volumes. Besides that, open repositories like SSRN and ZENODO are also quite vibrant, thus suggesting a trend towards preprint and open-access dissemination. Besides that, journals such as IEEE Access and Scientific Reports are leading the way in presenting the growing participation of Indian researchers in international, peer-reviewed venues, which is an indication of both their recognition and academic diversification in the cybersecurity field (see Table 3).

Institutional Affiliations in Cybersecurity Research

Based on the institutional analysis, it is clear that SRM Institute of Science and Technology is at the forefront of Indian cybersecurity research with a total of 194 publications. Afterward, Chitkara University and Lovely Professional University can be seen in the position of third and second respectively with 171 and 151 research papers. Besides these, well-known private universities like Amity, Chandigarh, and VIT-AP also show a significant research output which indicates the rising contribution of non-government institutions to cybersecurity research. The specialized departments such as the Department of Computer Science and Engineering and the School of Computer Science and Engineering are also very active academically and deeply engaged in the field (see Table 4). The predominance of multidisciplinary universities has, therefore, led to the conclusion that cybersecurity research in India is flourishing in technology-driven academic environments where there is an increasing institutional collaboration and knowledge exchange.

Keyword Analysis

The top of the list are the keyword distributions with “Computer Science” and “Computer Security” being the two major themes that indicate a technological and security aspect of the research to cybersecurity in India. A vast number of “Artificial Intelligence” and “Machine Learning” indicates the ever-increasing use of intelligent systems and predictive models in cybersecurity solutions. The presence of terms like “Internet Privacy,” “World Wide Web,” and “The Internet” indicates a strong focus on privacy and data protection in the digital environment. Furthermore, the use of terms like “Business” and “Engineering” demonstrates the different facets of technology to which the cybersecurity has been linked, i.e., technological advancements and the organizational and infrastructural applications (see Table 5). Therefore, the keyword plan reflects the convergence of AI-driven, privacy-focused, and multidisciplinary research trends in Indias cybersecurity landscape.

Table 3: Top Sources Contributing to Cybersecurity Research in India.

Rank	Source	Articles
1	Advances in Computational Intelligence and Robotics Book Series	107
2	Advances in Information Security, Privacy, and Ethics Book Series	88
3	SSRN Electronic Journal	81
4	Lecture Notes in Networks and Systems	76
5	IGI Global eBooks	73
6	IEEE Access	47
7	International Journal of Advanced Research in Science Communication and Technology	40
8	ZENODO (CERN European Organization for Nuclear Research)	38
9	Scientific Reports	35
10	International Journal for Research in Applied Science and Engineering Technology	31

DISCUSSION

The study shows a clear and rapid expansion of Indian cybersecurity research between 2016 and 2025, as reflected in the high annual growth rate and rising publication output. This upward trend aligns with earlier scientometric findings and corresponds with national initiatives such as Digital India, increased digital infrastructure, and growing policy focus on cyber defence.

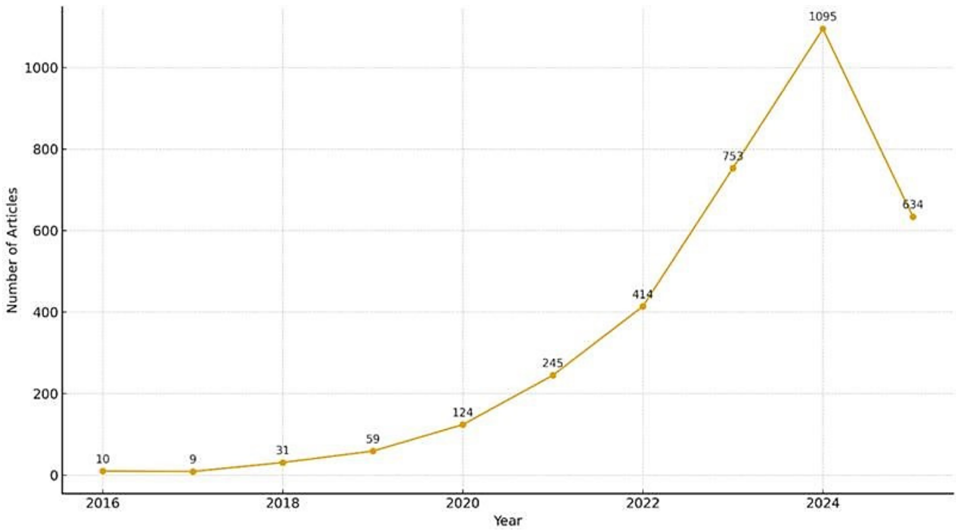

Figure 1: Year-wise growth of Cybersecurity publications in India (2016-2025).

Table 4: Top Contributing Affiliations in India.

Rank	Affiliation	Articles
1	SRM Institute of Science and Technology	194
2	Chitkara University Institute of Engineering and Technology	171
3	Lovely Professional University	151
4	Amity University	136
5	Chandigarh University	134
6	Department of Computer Science and Engineering	129
7	Hindustan Institute of Technology and Science	116
8	School of Computer Science and Engineering	116
9	VIT-AP University	109
10	Symbiosis International (Deemed University)	106

Keyword patterns-particularly the prominence of artificial intelligence, machine learning, and internet privacy-indicate a shift toward AI-driven cybersecurity themes, consistent with global research directions. The dominance of institutions like SRM Institute of Science and Technology, Chitkara University, and Lovely Professional University highlights the emergence of multidisciplinary hubs contributing significantly to this domain.

The reliance on book series, conference volumes, and open-access platforms suggests a preference for rapid knowledge dissemination and wider accessibility. Overall, the findings indicate that Indian cybersecurity research is becoming more interdisciplinary, collaborative, and internationally aligned, strengthening India's position in the global cybersecurity knowledge ecosystem.

Table 5: Top Keywords in Cybersecurity Research (2016-2025).

Rank	Keyword	Occurrences
1	Computer Science	3127
2	Computer Security	2499
3	Artificial Intelligence	1077
4	Business	808
5	World Wide Web	641
6	The Internet	612
7	Internet Privacy	602
8	Engineering	566
9	Machine Learning	511
10	Data Mining	376

SCOPE OF THE STUDY

The scope of this study is restricted to the examination of cybersecurity research publications that are affiliated with India and indexed in the OpenAlex database from 2016 to 2025. The study is confined to English-language documents of research publications, e.g., journal articles, book chapters, and conference papers. Through the use of bibliometric tools like R (Bibliometrix/ Biblioshiny) and Microsoft Excel, the research addresses various quantitative facets of the issue such as publication trends, authors with most publications, institution output, source impact, and keyword frequency. The study does not involve the qualitative content or full-text of the publications but mainly concentrates on the cognitive structure and collaboration patterns of the Indian cybersecurity research ecosystem. The defined scope acts to measure India's contribution to the global cybersecurity scholarly and to provide a platform for the new research areas that can be instrumental in the coordination of research and policy.

CONCLUSION

The bibliometric study of cybersecurity research in India from 2016 to 2025 exhibits a fast-changing and collaborative academic ecosystem in India, which is in line with global technological changes. The country has shown its ability to grow in numbers as well as in quality of research with a 58.57% yearly rate of increase and a strong trend of papers with multiple authors. The leading use of terms like computer science, artificial intelligence, and internet privacy points to the trend of the integration of intelligent technologies for solving ethical and social issues in digital security. Besides that, the SRM Institute of Science and Technology and Chitkara University have been identified as the productive academic centres, while the country's research visibility at the global level has been enhanced through the open-access mode of dissemination. This research confirms that India's cybersecurity scholarship is moving towards a more AI-driven, interdisciplinary, and globally connected model, which indicates its increasing academic and strategic value in securing the digital future, apart from being a leading edge of basic research.

ACKNOWLEDGEMENT

None.

ABBREVIATIONS

AI: Artificial Intelligence; **CSV:** Comma Separated Values; **IoT:** Internet of Things; **R:** Statistical Software/Programming Language; **RStudio:** Integrated Development Environment for R; **SSRN:** Social Science Research Network; **SRM:** SRM Institute of Science and Technology; **VIT-AP:** Vellore Institute of Technology - Andhra Pradesh; **WWW:** World Wide Web.

CONFLICT OF INTEREST

The author declares that there is no conflict of interest.

AUTHOR CONTRIBUTION

Kishore Dey is the sole author of this manuscript and undertook all responsibilities, including:

- Conceptualization and research design,
- Data extraction from OpenAlex,
- Data cleaning and preprocessing using MS Excel,
- Bibliometric analysis using R (Bibliometrix/Biblioshiny),
- Interpretation of results and preparation of figures/tables,
- Writing, revising, and finalizing the manuscript.

No other individuals contributed to the research, analysis, or writing.

SUMMARY

This study explores the cognitive and collaborative landscape of cybersecurity research in India (2016-2025) through a bibliometric analysis of 3,374 publications indexed in the OpenAlex database. Using R (Bibliometrix/Biblioshiny) and Microsoft Excel, it identifies publication trends, prolific authors, top institutions, and thematic focuses. Results reveal an annual growth rate of 58.57%, indicating a rapidly expanding and interdisciplinary research environment. The dominance of journal articles (66.4%) and book chapters (24.8%) shows India's dual focus on scholarly and collaborative dissemination. SRM Institute of Science and Technology, Chitkara University, and Lovely Professional University are the leading contributors, while keywords such as artificial intelligence, machine learning, and internet privacy highlight the nation's AI-driven and ethical research orientation. Overall, India's cybersecurity scholarship demonstrates global collaboration, technological innovation, and a growing alignment with worldwide digital security priorities.

REFERENCES

Albahri, O. S., & Alamoodi, A. H. (2023). Cybersecurity and artificial intelligence applications: A bibliometric analysis based on Scopus database. Mesopotamian Journal of CyberSecurity, 2023, 158–169. https://doi.org/10.58496/MJCSC/2023/018

Coman, E., Coman, C., Alexandrescu, M. B., & Bilţi, R.-S. (2025). Mapping the frontiers of cybersecurity and data protection: Insights from a bibliometric study. Electronics, 14(19), 3769. https://doi.org/10.3390/electronics14193769

Elango, B., Matilda, S., Martina Jose Mary, M., & Arul Pugazhendhi, M. (2023). Mapping the cybersecurity research: A scientometric analysis of Indian publications. Journal of Computer Information Systems, 63(2), 293–309. https://doi.org/10.1080/08874417.2022.2058644

Ganji, K., & Afshan, N. (2025). A bibliometric review of Internet of things (IoT) on cybersecurity issues. Journal of Science and Technology Policy Management, 16(6), 984–1002. https://doi.org/10.1108/JSTPM-05-2023-0071

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: Bibliometric analysis of the literature. Journal of Medical Internet Research, 21(2), Article e12644. https://doi.org/10.2196/12644

Loan, F. A., Bisma, B., & Nahida, N. (2022). Global research productivity in cybersecurity: A scientometric study. Global Knowledge, Memory and Communication, 71 (4/5), 342–354. https://doi.org/10.1108/GKMC-09-2020-0148

Nayak, S., Mashroofa, M. M., Parida, D. K., & Saini, P. K. (2024). Mapping the cyber security research horizon in India: An in-depth analysis of current trends and global perspectives. Marathwada Itihas Parishad – History Research Journal, 31(5), 193–201.

Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. Journal of Financial Crime, 30(6), 1736–1754. https://doi.org/10.1108/JFC-11-2022-0287

Purnama, Y., Asdlori, A., Ciptaningsih, E. M. S. S., Kraugusteeliana, K., Triayudi, A., & Rahim, R. (2024). Machine learning for cybersecurity: A bibliometric analysis from 2019 to 2023. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15(4), 243–258. https://doi.org/10.58346/JOWUA.2024.I4.016

Sulich, A., Zema, T., & Kulhanek, L. (2023). Towards a secure future: A bibliometric analysis of the relations between cybersecurity and sustainable development. In Procedia Computer Science. Elsevier, 225, 1448–1457. https://doi.org/10.1016/j.procs.2023.10.133

Zainal Abidin, N., Sri Ramalu, S., Nadarajah, G., & Anuar, A. (2025). A bibliometric analysis of cybersecurity behaviour in organization. Sage Open, 15(3). https://doi.org/10.1177/21582440251361635

Cite this article: Dey K. The Cognitive Cartography of Cybersecurity: India's Knowledge Pathways and Scholarly Networks. Info Res Com. 2025;2(3):355-60.