Mapping Global Research Trends in Cybersecurity and Artificial Intelligence: A Bibliometric Analysis (2008–2025)

HAFZA TARANNUM
5th Semester BCA Student, Department of Computer Applications, BET Sadathunnisa Degree College

Abstract: ***This study presents a bibliometric assessment of existing research connecting cybersecurity and artificial intelligence. It explores leading authors, prominent journals, institutional affiliations, contributing countries, emerging themes, research trends, and patterns of international collaboration. Data were collected from the Web of Science database and initially 342 publications retrieved, after applying inclusion and exclusion criteria, 312 relevant records were extracted in BibTeX format for analysis. The Biblioshiny tool within the R-package facilitated the data examination. Results reveal a sharp growth in academic output on the intersection of cybersecurity and AI. Core keywords such as "Cybersecurity," "Artificial Intelligence," "Machine Learning," and "Intrusion Detection" appeared most frequently. Among the contributors, Samtani S emerged as the most productive author, while the United States ranked highest in publication count, global citations, and collaborative efforts. The analysis further highlights major thematic areas and emerging topics. Overall, this study offers valuable insights into the evolving research landscape of cybersecurity and AI, helping scholars identify influential contributors and address ongoing challenges in mitigating cyber threats.***

Index Terms- Cybersecurity, Artificial Intelligence (AI), "Machine Learning", Bibliometric studies, Biblioshiny web tool.

I. INTRODUCTION

Cybersecurity and Artificial Intelligence (AI) have become pivotal components of the modern technological environment, shaping new frontiers and offering remarkable possibilities across multiple sectors (Carrasco, 2024; Albahri & Al-Amoodi, 2024). AI technologies, particularly those utilizing Machine Learning (ML) and Deep Learning (DL), demonstrate strong potential in addressing cybersecurity challenges by improving the detection, classification, and prevention of cyber threats (Makawana et al., 2017). These technologies play a crucial role in protecting computer systems, networks, and digital data from unauthorized access, misuse, or damage (Awasthi & Goel, 2024). With continuous technological advancement, the scale and sophistication of cyberattacks have increased significantly. Modern threats now encompass issues such as cyberbullying, identity theft, wireless sensor network attacks, and vulnerabilities in digital devices and autonomous systems (Chetry & Sharma, 2023).

A. Research Questions

RQ1. In what ways has research evolved in cybersecurity and artificial intelligence evolved over time?
RQ2. Which authors, publication sources, and institutions demonstrate the greatest influence and citation impact within the field of cybersecurity and artificial intelligence? RQ3. What are the thematic evolution of cybersecurity and artificial intelligence studies using keyword cooccurrence and mapping analyses?
RQ4. What emerging themes and future research directions can be identified in the evolving landscape of cybersecurity and artificial intelligence studies?

II. LITERATURE SURVEY

The current study examines the evolution of research, major contributors, publication outlets, and institutional involvement in the field of cybersecurity and artificial intelligence. It highlights citation impacts, thematic progressions, emerging research areas, and potential future directions within this domain.

Bibliometric analysis has proven to be a powerful approach for mapping research productivity, collaboration networks, and the intellectual structure of a discipline. Accordingly, this study applies bibliometric methods on metadata research and to understand the convergence of cybersecurity and AI, emphasizing their growing role in protecting the digital environment (Taj et al., 2024;

Subaveerapandiyan et al. (2025)).

Previous investigations have adopted similar approaches. For instance, Makawana et al. (2017) analyzed bibliometric data from recent publications focusing on the use of machine learning in cybersecurity. Their findings indicated that, between 2015 and 2016, the dominant research themes centered on detecting malicious patterns and defending against cyber adversaries.

Likewise, Khurana (2024) conducted a bibliometric analysis of cybersecurity trends using the Web of Science database. Their study revealed that the automation of cyber-behavioral analysis through machine learning has emerged as a key focus area in contemporary cybersecurity research.

Cojocaru and Cojocaru (2022) also emphasized that research in cybersecurity is still in its formative stage, yet it is expected to become a critical component in an increasingly digital and information-driven society.

III. METHODOLOGY

A. RESEARCH DESIGN

This research adopts a bibliometric methodology to explore the growth and influence of scholarly work related to Cybersecurity and Artificial Intelligence. The bibliometric approach, being quantitative in nature, enables the assessment of publication patterns, citation behavior, and collaborative relationships within the research community. Through this method, the study systematically maps the academic landscape of Cybersecurity and AI by examining core indicators such as yearly publication output, author productivity, citation performance, institutional partnerships, and the evolution of keyword usage.

B. DATA COLLECTION

The dataset for this study was retrieved from the Web of Science database on 03rd October, 2025. The search strategy used the following query: (TI=(cybersecurity and artificial intelligence) OR TI=(cybersecurity and AI))
AND (DT==("ARTICLE" OR "PROCEEDINGS PAPER" OR "REVIEW" OR "BOOK CHAPTER" OR "BOOK")) The search yielded 312 documents, ensuring a comprehensive coverage of scholarly works related to *Cybersecurity* and *Artificial Intelligence*.

C. INCLUSION AND EXCLUSION CRITERIA

To ensure the accuracy and relevance of the dataset, the analysis included only peer-reviewed journal articles, conference papers, books, and book chapters. Nonscholarly materials such as editorials, commentaries, letters, and duplicate records were excluded. The finalized dataset covered publications from 2008 to October 3, 2025, providing a broad time frame to observe the developmental trends in Cybersecurity and Artificial Intelligence research.

D. DATA ANALYSIS

Data analysis was performed using the R-based *Bibliometrix* package and VOSviewer for visualizing research networks. The dataset was sourced exclusively from the Web of Science, ensuring data credibility.

Established bibliometric principles, including Bradford's
Law for key sources, Lotka's Law for author productivity, and co- citation analysis, were applied to enhance analytical validity. However, the study is limited to Web of Science–indexed records, which may omit relevant works from other databases. Moreover, bibliometric indicators may not fully reflect the qualitative dimensions of Cybersecurity and Artificial Intelligence research (Taj et al., 2024; Subaveerapandiyan et al., 2025).

IV. FINDIGNS AND DISCUSSIONS

The findings underscore the relevance of the present study, which analyzed research outputs on Cybersecurity and Artificial Intelligence from 2018 to 2025, including early-access publications from 2026. A total of 312 documents were identified, originating from 232 sources and authored by 1,121 researchers. Among these, 45 were single-authored works, while around 30% involved coauthorship. The dataset included approximately 1,000 unique keywords, with an average document age of 1.54 years and an average citation rate of 7.93 per paper. Detailed insights are illustrated in Figure 1.

Figure 1. Overview on Cybersecurity and Artificial Intelligence

Table 1. Annual Scientific Production

Year	Articles	Percentage
2018	5	2
2019	13	4
2020	16	5
2021	12	4
2022	16	5
2023	46	15
2024	99	31
2025	105	34
Total	312	100

Table 2. Average Citations Per Year

Year	MeanTCperArt	N	MeanTCperYear	Citable Years
2018	12.40	5	1.55	8
2019	16.15	13	2.31	7
2020	16.81	16	2.80	6
2021	7.92	12	1.58	5
2022	30.31	16	7.58	4
2023	15.98	46	5.33	3
2024	4.92	99	2.46	2
2025	1.27	104	1.27	1

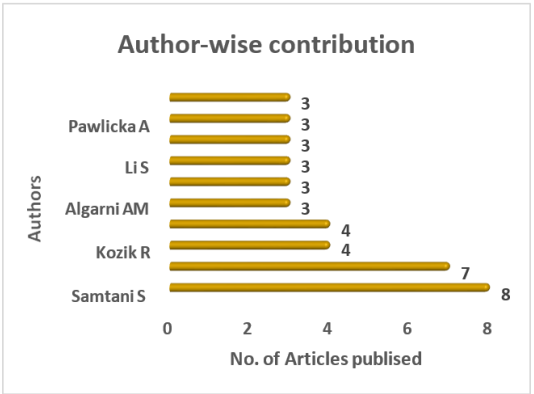

Figure 2. Prolific Author Contribution

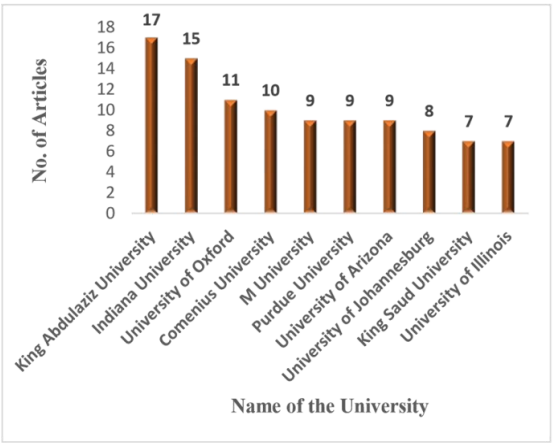

Figure 3. University-wise Contribution

Table 3. More Relevant Sources

Sources	Articles	Percent
IEEE Access	23	7.4
Applied Sciences-Basel	7	2.2
Electronics	5	1.6
Artificial Intelligence Review	4	1.3
Information and Computer Security	4	1.3
Journal of Cybersecurity And Privacy	4	1.3
Scientific Reports	4	1.3
AI in Cybersecurity	3	1
CMC-Computers Materials & Continua	3	1
Future Generation Computer Systems-The International Journal of Escience	3	1

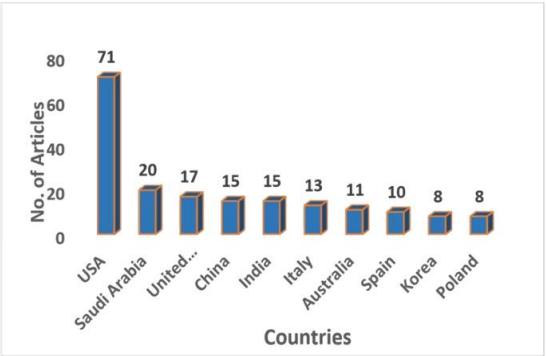

Figure 4. Countries-wise contribution

Table 4. Most Influential Works

Most Influential Works in Cybersecurity and Artificial Intelligence			
Paper	Total Citations	TC per Year	Normalized TC
GUPTA M, 2023, IEEE ACCESS	245	81.67	15.33
KAUR R, 2023, INF FUSION	136	45.33	8.51
ABDULLAHI M, 2022, ELECTRONICS	131	32.75	4.32
TADDEO M, 2019, NAT MACH INTELL	98	14	6.07
CAPUANO N, 2022, IEEE ACCESS	91	22.75	3
ZEADALLY S, 2020, IEEE ACCESS	89	14.83	5.29
RODRIGUES ARD, 2022, RES INT BUS FINANC	63	15.75	2.08
CHARMET F, 2022, ANN TELECOMMUN	45	11.25	1.48
SAMTANI S, 2020, ACM TRANS MANAG INF SYST	43	7.17	2.56
POOYANDEH M, 2022, APPL SCI-BASEL	42	10.5	1.39

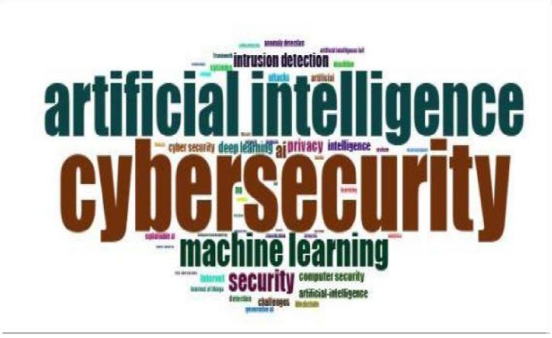

Figure 5. Most Frequent Keywords

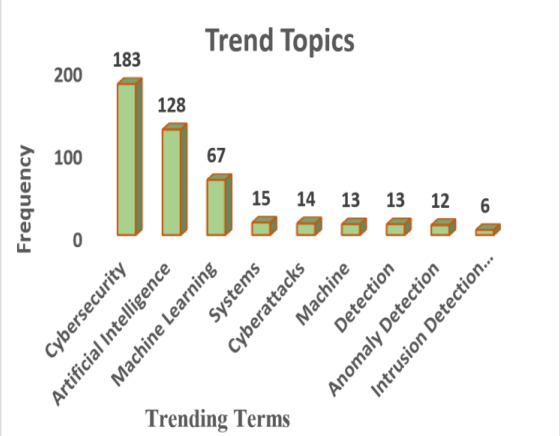

Figure 6. Emerging Trends

V. CONCLUSION AND FUTURE DIRECTIONS

Cybersecurity and Artificial Intelligence (AI) play a vital role in protecting digital infrastructures from evolving threats. Beyond technological solutions, maintaining a secure digital environment requires continuous awareness, collaboration, and preparedness across sectors. This study used bibliometric analysis to explore publication trends, key themes, influential contributors, and international collaborations in the field. The results highlight emerging research opportunities in areas such as blockchain-based security, AI-driven defense systems, intelligent threat detection, AI chatbots, early cybercrime prediction, digital forensics, and malware identification. Continued innovation and interdisciplinary research are essential to strengthen global cybersecurity resilience.

REFERENCES

[1] J. G. Carrasco Ramírez and Md. M. Islam, "Utilizing Artificial Intelligence in Real-World Applications," JAIGS, vol. 2, no. 1, pp. 14–19, Feb. 2024, doi: 10.60087/jaigs.v2i1.p19.

[2] O. S. Albahri and A. H. Al Amoodi, "Cybersecurity andArtificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database," *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 158–169, Sept. 2023, doi: 10.58496/MJCSC/2023/018.

[3] P. R. Makawana and R. H. Jhaveri, "A Bibliometric Analysis of Recent Research on Machine Learning for Cyber Security," in Intelligent Communication and Computational Technologies, vol. 19, Y.-C. Hu, S. Tiwari, K. K. Mishra, and M. C. Trivedi, Eds., in Lecture Notes in Networks and Systems, vol. 19. , Singapore: Springer Singapore, 2018, pp. 213–226. doi: 10.1007/978-981-10-5523-2_20.

[4] A. Awasthi and N. Goel, "An Approach for Efficient and Accurate Phishing Website Prediction Using Improved ML Classifier Performance for Feature Selection," *IJERR*, vol. 40, no. Spl Volume, pp. 73–89, June 2024, doi: 10.52756/ijerr.2024.v40spl.006.

[5] A. Chetry and U. Sharma, "Anonymity in decentralized apps: Study of implications for cybercrime investigations," *IJERR*, vol. 32, pp.195–205,Aug. 2023, doi:10.52756/ijerr.2023.v32.017.

[6] P. Khurana, S. Narula, N. Tiwari, R. Kapoor, and M. Arora, "Mapping the Cybersecurity Research: A Comprehensive Bibliometric Analysis," IJERR, vol. 46, pp. 202–211, Dec.

2024, doi: 10.52756/ijerr.2024.v46.016.

[7] Taj, Amreen., Vyas, A. & Kumar, A. (2024). Interdisciplinary Research on the Metaverse: General and Library Perspectives on Bibliometric Insights. International Journal of Social Impact, 9(1), 222- 242. DIP: 18.02.024/20240901, DOI: 10.25215/2455/0901024

[8] Subaveerapandiyan A, Taj, Amreen & Aravind R. Nair (2025): Advancing Open Science: A Bibliometric Study of Scholarly Metadata Research (1995–2024), Science & Technology Libraries, DOI: 10.1080/0194262X.2025.2517089

[9] I. Cojocaru and I. Cojocaru, "A bibliomeric analysis of cybersecurity research papers in Eastern Europe: Case study from the Republic of Moldova," *ocg*, vol. 335, pp. 151–162, Mar.2022, doi: 10.24989/ocg.v335.12