DOI: http://dx.doi.org/10.26483/ijarcs.v16i4.7298

Volume 16, No. 4, July-August 2025

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: A DECADE OF RESEARCH TRENDS AND DEVELOPMENTS THROUGH BIBLIOMETRIC ANALYSIS

Saravanamuthu M, Shaik Shaziya*, Patan Sadiqunnisa, Palamaneru Nataraj Kumar Sasi Priya, Shafiyakousar Pathan, Kutagolla Shajida

Madanapalle Institute of Technology & Science, Madanapalle, Andhra Pradesh,India

Abstract: This study presents a comprehensive bibliometric analysis of the research landscape at the intersection of Artificial Intelligence (AI) and cybersecurity over the period 2017–2024. With an emphasis on deep learning (DL) and natural language processing (NLP), the analysis utilizes data sourced from the Scopus database and analyzed through VOSviewer and Biblioshiny. The dataset includes 2,692 publications, revealing a steep growth in scholarly output since 2018 and highlighting key contributions, collaborative networks, and influential research themes. Keyword co-occurrence and thematic mapping show that while deep learning and intrusion detection remain dominant, emerging areas such as federated learning and adversarial machine learning indicate a shift towards decentralized and adaptive cybersecurity approaches. The findings underline the dynamic and interdisciplinary nature of AI-driven cybersecurity research, offering vital insights for scholars, industry experts, and policymakers to shape future directions in this fast-evolving field.

Keywords: Artificial Intelligence, Cybersecurity, Deep Learning, Natural Language Processing, Intrusion Detection.

INTRODUCTION

Over the past few years, the use of Artificial Intelligence (AI) in cybersecurity has been a revolutionary method in meeting the escalating complexity and volume of cyber threats[1]. Following the explosive growth of digitalization, cloud computing, and devices, conventional rule-based and signature-based security solutions have not been effective enough to counter complex persistent threats, zero-day threats, and dynamic malware. Consequently, AI, and more specifically methodologies like deep learning (DL) and natural language processing (NLP), has emerged as a primary facilitator of smart, adaptive, and real-time cybersecurity solutions[2].The importance of AI in cybersecurity is also boosted by its ability to scan enormous amounts of data to identify threats, automate the response, and learn from past threats to strengthen subsequent defences [3].In addition, AI frameworks have been found effective in decreasing the time required to detect and neutralize threats, which is essential in the changing threat environment [4].

Deep learning models like convolutional and recurrent neural networks are well-suited for intrusion detection and malware tagging by detecting patterns in big unstructured data[5]. Natural language processing (NLP) also assists in early threat detection through processing of unstructured threat information, e.g., phishing emails and social media posts. Combining all these AI solutions greatly helps strengthen cybersecurity readiness and resistance to emerging threats[6].In light of the recent surge of interest in the field of AI and cybersecurity, a significant amount of academic research has been produced in the last ten years. Nevertheless, even with this burgeoning body of research, limited studies have documented the intellectual structure, publication patterns, collaboration networks, and thematic focus areas of this field. A recent bibliometric study has given a systematic, quantitative approach to investigate these dimensions, providing insight into the history and present status of the discipline[7].

The aim of this research is to provide an in-depth bibliometric review of articles from the years 2017 through 2024 that investigate the use of deep learning and NLP in cyber security. Based on Scopus as the dataset and the use of tools such as VOSviewer and Biblioshiny, the article identifies top authors, organizations, topics, and upcoming trends and offers a useful guide towards future research in AI-based cyber security.

OBJECTIVE OF THE STUDY

The goal of this research is to chart the growth and trends of Artificial Intelligence application research in cybersecurity from 2017 until 2024 based on bibliometric analysis.

It will seek to examine trends in annual publications, determine dominant thematic clusters such as intrusion detection and deep learning, and point out rising subjects such as federated learning and adversarial machine learning.

The research also aims to map keyword patterns of co-occurrence and strategic themes to gain insights into intellectual and thematic development in the field.

RESEARCH METHODOLOGY

A. Data Retrieval and Selection

The research has been done to examine the research production in the field of Artificial Intelligence applications in cybersecurity as evident through peer-reviewed journal publications in the Scopus database. It aims to examine global research trends in this interdisciplinary area over the time frame of 2017 to 2024.The relevant bibliographic data

© 2023-2025, IJARCS All Rights Reserved

was extracted from Scopus, a leading multidisciplinary abstract and citation database covering high-impact academic journals, conference proceedings, and review articles across scientific disciplines and geographies. Scopus was selected for its robust indexing of computer science and engineering literature, which aligns well with the scope of this study. An article-level search was conducted on a structured Boolean query based on keywords of "deep learning," "natural language processing," and "cybersecurity." Filters were placed to limit the results to journal articles and reviews, English language, published in the chosen subjects of interest. The dataset was captured in the first week of June 2025 to maintain consistency and reduce the impact of continuous database updates. The exported dataset was then examined using bibliometric software such as VOSviewer and Biblioshiny (RStudio interface), which facilitated network visualization and thematic investigation of the research output.

B. Data Analysis and Visualization

Given that the interest of the current study is to investigate the development and thematic pattern of research trends in the domain of Artificial Intelligence (AI) for use in cybersecurity, the examination incorporates research articles that involve terminology specific to both AI and cybersecurity. To evaluate the trends in year-wise publication and research activity, the search strategy employed a sensitive Boolean query designed to target co-occurrence of the major terms like 'deep learning,' 'natural language processing,' 'cybersecurity,' 'cyber security,' and 'network security' in Title, Abstract, and Keyword fields of publications. In order to have a tight dataset, the search was limited to journal articles and review papers in English from 2017 to 2024. Subject fields were restricted to Computer Science, Engineering, Decision Sciences, and related disciplines, and only Scopus-indexed publications were taken into account.The bibliometric analysis entailed publication number by year evaluation, collaboration and co-authorship behaviors, keyword frequency and co-occurrence, and thematic development of research fields[5]. Author-supplied keywords were carefully examined in order to determine the most productive and impactful research topics in the field. The findings of the analysis have been organized methodically both in visual and tabular forms. Visualization software like VOSviewer was employed in producing keyword co-occurrence maps and collaboration networks, whereas Biblioshiny (RStudio) supported annual trend analysis, thematic mapping, and trend topic exploration[6]. These tools assisted in determining key research clusters, novel themes, and the evolving path of AI-fueled cybersecurity research.

RESULTS AND DISCUSSION

4.1 Descriptive Statistics

The bibliometric dataset in table 1 is comprised of 2,692 documents that were indexed during the years 2017 to 2025. They were published in 513 different sources, which include peer-reviewed journals and academic proceedings. All chosen publications are in the English language and from core scientific fields like Computer Science, Engineering, Decision Sciences, and Information Systems. Types of documents considered are both review papers and research articles, consistent with the study goal of assessing scientific impact and thematic progression. The dramatic surge in publications after 2018 reflects the rapidly increasing use of AI methods, particularly deep learning, in cybersecurity research. The predominance of documents published in high-impact journals reflects high academic and practical significance. This development marks a strategic move towards intelligent, automated threat detection and prevention solutions.

Table 1 Summary Statistics of AI-Cybersecurity Research Publications (2017–2025)

Description	**Results**
Main Information About Data	
Timespan	2017:2025
Sources (Journals, Books, etc)	513
Documents	2692
Annual Growth Rate %	-13.97
Document Average Age	2.46
Average citations per doc	36.73
References	125211
DOCUMENT CONTENTS	
Keywords Plus (ID)	10167
Author's Keywords (DE)	5442
AUTHORS	
Authors	7557
Authors of single-authored docs	107
AUTHORS COLLABORATION	
Single-authored docs	115
Co-Authors per Doc	4.26
International co-authorships %	37.3
DOCUMENT TYPES	
Article	2499
Review	193

4.2 Annual Scientific Production

Figure 1 The yearly scientific output between 2017 and 2024 depicts a steep incline, an indication of growing academic and industry interest in the intersection of Artificial Intelligence and cybersecurity. During 2017, the field recorded 10 publications, which drastically rose over the subsequent years, reaching its peak at 904 during 2024. The spike after 2018 is consistent with emerging breakthroughs in deep learning and mounting needs for automated threat detection systems. The steep increase from 2020 and beyond reflects the mainstreaming of AI deployments in security infrastructure

© 2023-2025, IJARCS All Rights Reserved

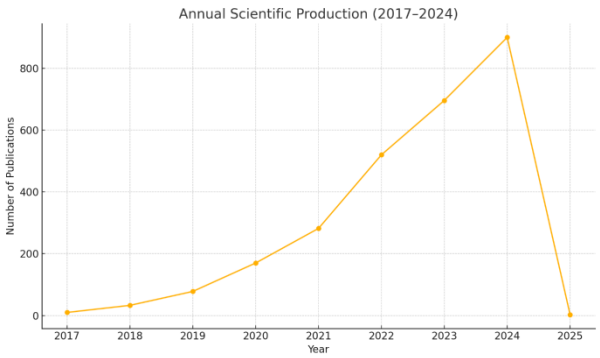

Figure 1: Annual scientific production showing the growth of AI in cybersecurity literature

4.3 Thematic Evolution and Strategic Mapping

Figure 2 illustrates the strategic thematic map created using Biblioshiny , which classifies research themes according to their centrality (relevance) and density (development). Four quadrants group themes as Motor Themes, Basic Themes, Niche Themes, and Emerging / Declining Themes.

In the Motor Themes quadrant, themes like "cybersecurity," "learning systems," and "intrusion detection" are well-developed and core, representing the most mature and most actively studied themes. Basic Themes like "deep learning," "network security," and "Internet of Things" are basic foundation themes with wide interest but s hallower development depth. Emerging Themes like "reinforcement learning" and "deep reinforcement learning" are newer or currently less explored themes. In contrast, Niche Topics such as "antennas" and "aircraft detection" are well developed but narrow in scope or application to the general discipline.

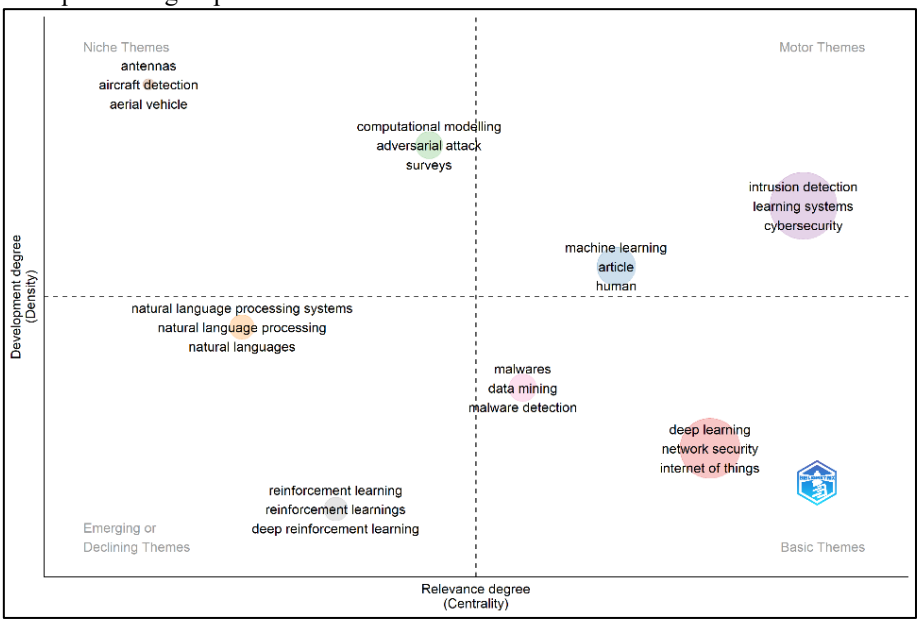

Figure 2. Strategic Thematic Map showing keyword positioning by centrality and density.

4.4 Trend Topics

Trend topic analysis visualized Figure 3 using Biblioshiny demonstrates the way important terms have changed over time. During the years 2019-2021, the research was predominantly focused on core methods like "neural networks," "decision trees," and "intrusion detection." Starting in 2022, it is apparent that there is an uptick in complex and technical subjects like "federated learning," "cyber attacks," and "adversarial machine learning," indicating the area's quick adaptation to developing cyber threats."Deep learning" and "network security" are the most frequent and persistent, emphasizing their continued relevance over the period observed. The emergence of new trends like "state-of-the-art approaches," "zero-trust architecture," and privacy-conscious learning processes indicate the directions of coming research that are proactive and adaptive in nature and aim towards cybersecurity models.

© 2023-2025, IJARCS All Rights Reserved

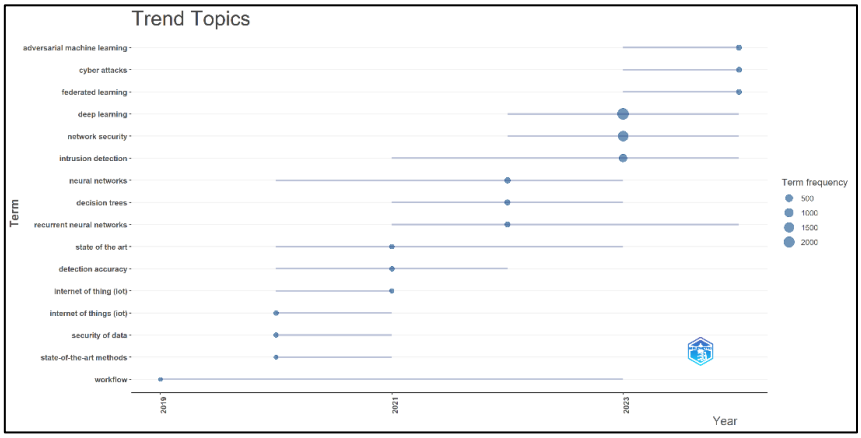

Figure 3: Trend topic timeline illustrating the evolution and frequency of key AI-cybersecurity terms (2019–2024).

4.5 Keyword Co-occurrence Analysis – Interpretation

The keyword co-occurrence map shows the thematic organization of AI research in cybersecurity as frequently mentioned terms in co-occurrence within the 2,692 publications examined. The visualization, created with VOSviewer, shows various dense clusters of keywords, representing different research avenues and thematic connections. At the middle of the map is "deep learning", the most prominent and most connected keyword. Its core location and node size emphasize its root position in AI-based cybersecurity applications. It is closely associated with "cybersecurity", "intrusion detection", and "recurrent neural networks", implying that these are some of the most heavily researched and significantly interconnected topics in the area.

Cluster analysis has highlighted four prominent clusters including:

Red Cluster: Concerned with deep learning and related subfields about deep reinforcement learning, neural networks, and application in IoT security, authentication and vehicle-to-vehicle communications.

Blue Cluster: Concerned with intrusion detection, attack detection, and LSTM models all of which display research situated in sequential data analytics, and anomaly detection systems.

Green Cluster: Covers natural language processing, adversarial attacks, feature extraction, and computational modelling and highlights the use of AI to assist in interpreting written threat intelligence and improving model robustness.

Orange Cluster: Focuses on malware detection, phishing, static analysis, and random forest identified as old-fashioned forms of machine learning, emphasising traditional machine learning implementations of cybersecurity domains.

In addition to the larger clusters, peripheral words convey increasing interest in model security, generalization, and the detection of zero-day threats, shown in text of words like "adversarial attacks", "feature fusion", and "zero-day detection".

The clusters' complex interchangeable of keywords identified a high degree of interdisciplinarity where AI subfields including NLP, reinforcement learning, and deep neural networks are being used together in efforts to meet current cybersecurity needs. The visual map reinforces the notion that deep learning, intrusion detection and malware classification are hotspots, whilst newer areas of adversarial robustness and threats to autonomous systems are on the radar but not yet intensely researched.

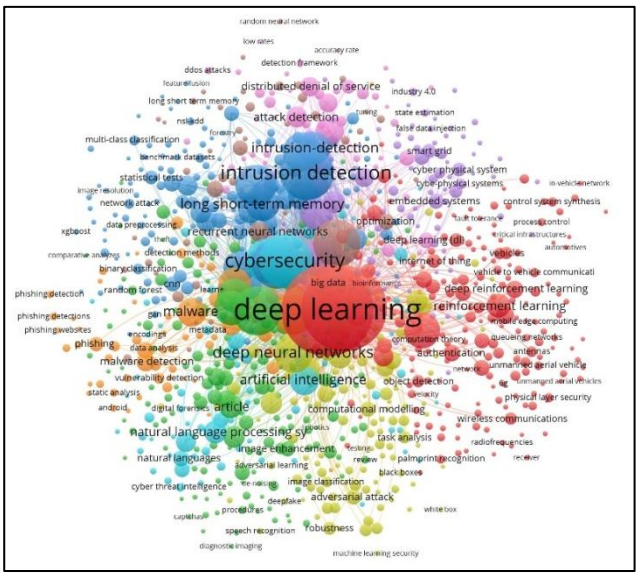

Figure 4: Keyword Co-occurrence

FINDINGS

The purpose of the current study was to assess the changes in growth and themes of the AI in Cybersecurity research literature between 2017 - 2024. The universe of studies (a total of 2,692) retrieved contained several types of studies, but focused on articles and review articles that are indexed in the Scopus database. The study wanted documents that relate to some keywords and/or situations such as: “deep learning”, “natural language processing”, “cybersecurity”, “network security” (and many dialects of those as well). The study shows that after (2018), there was a significant increase in academic output and appears to have directly relates to the increasing importance of AI-based strategies to tackle complex cyber security issues. When looking at the co-occurrence analysis, “Deep Learning” is the most important and occurs most frequently, followed by “intrusion detection”, “cybersecurity” then “recurrent neural networks”. All of these words are well supported in any of the AI - Cybersecurity literature and are basic to researchers in this area.

© 2023-2025, IJARCS All Rights Reserved

Thematic analysis further qualified “cybersecurity” and “learning systems” as a fully developed, and most relevant (motor themes), whereas “deep learning” and “network security” show foundational structures but were also less tightly formed (basic themes). Emerging keywords such as “federated learning” and “adversarial machine learning” indicate potential future themes in more decentralized models versus unified (monolithic) AI models for security (of infrastructure).

The analysis of the theme trends shows a transition from more traditional approaches (such as "neural networks" and "decision trees") towards more cutting-edge AI approaches (such as "federated learning" and "adversarial machine learning") indicating a shift toward models with adaptable and scalable, and privacy-preserving characteristics in a changing cyber threat landscape.

Overall, the findings signal an energetic and cross-discipline research space with deep learning and intrusive detection showing strong relevance, and federated learning and adversarial learning demonstrating strong promise going forward.

CONCLUSION

This work offers a comprehensive bibliometric review examining the area of artificial intelligence (AI) applied to the field of cybersecurity based on literature published between 2017 and 2024. The review examined 2,692 documents available in the Scopus database and reported the strong growth, thematic evolution, and intellectual structure of quick-developing field that remains interdisciplinary. The growth result showed a clear upward trend in publication output, with a surge of articles published starting in 2018, and coverage in the three dominant areas of: deep learning, intrusion detection, and cybersecurity. The keyword co-occurrence and trending topic analyses show movement away from classic machine learning models towards better, more advanced and adaptive, approaches in the form of federated learning (FL), adversarial machine learning (AML), and deep reinforcement learning (DRL). These changing topics also highlight the need for scalable, decentralized, and robust AI models to address the changing sophistication of cyber-threats. In addition, using thematic mapping found that cybersecurity, learning systems developed as highly developed motor themes, identified as foundational and well-explored areas were deep learning (DL) and network security.The rise of new clusters and terms in recent years confirms the ongoing evolution of the field into new areas such as privacy-aware AI, autonomous detection systems, and smart threat intelligence extraction with NLP. In addition, the research depicts high levels of international collaboration and interdisciplinary collaboration, with the United States, China, and India leading contributions. It also notes that over 7,500 contributing authors and average co-authorship of 4.26 indicate the collaborative nature of the research field. To summarize, the results demonstrate that AI-driven cybersecurity is a dynamic, rapidly evolving research field generating increasing significance to academia, industry, and society. This study was intended to lay groundwork for researchers, policymakers, and practitioners attempting to understand the development of AI applications in the cybersecurity field and ultimately delineate new directions for future research and innovation.

REFERENCES

[1] F. Jimmy, “Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses,” *International Journal of Scientific Research and Management (IJSRM)*, vol. 9, no. 02, pp. 564–574, Feb. 2021, doi: 10.18535/ijsrm/v9i2.ec01.

[2] Rahul Kumar Jha, “Strengthening Smart Grid Cybersecurity: An In-Depth Investigation into the Fusion of Machine Learning and Natural Language Processing,” *Journal of Trends in Computer Science and Smart Technology*, vol. 5, no. 3, pp. 284–301, Sep. 2023, doi: 10.36548/jtcsst.2023.3.005.

[3] Dr. W. S. Ismail, “Threat Detection and Response Using AI and NLP in Cybersecurity,” *Journal of Internet Services and Information Security*, vol. 14, no. 1, pp. 195–205, Mar. 2024, doi: 10.58346/JISIS.2024.I1.013.

[4] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, “A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience,” *Sensors*, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

[5] U. Ahmed *et al.*, “Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering,” *Sci Rep*, vol. 15, no. 1, p. 1726, Jan. 2025, doi: 10.1038/s41598-025-85866-7.

[6] B. Prima and M. Bouhorma, “USING TRANSFER LEARNING FOR MALWARE CLASSIFICATION,” *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLIV-4/W3-2020, pp. 343–349, Nov. 2020, doi: 10.5194/isprs-archives-XLIV-4-W3-2020-343-2020.

[7] O. S. Albahri and A. H. AlAmoodi, “Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database,” *Mesopotamian Journal of CyberSecurity*, vol. 2023, pp. 158–169, Sep. 2023, doi: 10.58496/MJCSC/2023/018.

© 2023-2025, IJARCS All Rights Reserved