Artificial Intelligence in Cybersecurity: A Bibliometric Analysis of Recent Advances and Emerging Trends

SILVESTRU Cătălin-Ionuț[1], FIRULESCU Alexandru-Cristian[1], IORDOC Dumitru-Georgian[1], CRĂCAN (ȘERBU) Elena-Irina[1], Stoica Mihai-Alexandru[1]

[1]Faculty of Economic Cybernetics, Statistics and Informatics, Bucharest University of Economic Studies, 010374 Bucharest, Romania
[2]Faculty of Industrial Engineering and Robotics, National University of Science and Technology "Politehnica" Bucharest, 060042 Bucharest, Romania

Abstract

Cybersecurity faces mounting challenges as digital systems grow more complex and interconnected, necessitating innovative approaches to counter escalating threats. This study explores the evolving research landscape where artificial intelligence (AI), particularly machine learning and deep learning, emerges as a critical enabler for detecting, mitigating, and preventing cyberattacks. Utilizing a bibliometric analysis of over 10,000 publications from 2022 to 2024, this research examines key trends, thematic priorities, and collaborative dynamics shaping AI-driven cybersecurity solutions. Data collected from the Web of Science Core Collection was analyzed using Biblioshiny to map intellectual foundations, identify influential sources, and construct co-occurrence networks of core concepts. The findings reveal a field dominated by datacentric methodologies, with terms like "learning," "data," and "model" highlighting the integration of AI into anomaly detection, predictive analytics, and system defense. Geographic analysis underscores China's leadership in research productivity, complemented by strong international collaboration from countries like the United Kingdom and Australia. Thematic clusters highlight emerging concerns such as IoT security, privacy protection, and cloud resilience, emphasizing the ethical and practical implications of AI applications. This study demonstrates that AI is fundamentally reshaping cybersecurity, enabling scalable and adaptive solutions to meet evolving threats. Future research must continue fostering interdisciplinary collaboration and ethical innovation to ensure AI technologies remain robust and equitable tools in safeguarding digital ecosystems.

Keywords: artificial intelligence, cybersecurity, machine learning, data privacy, IoT security

1. Introduction

The increasing complexity and interconnectedness of digital systems have brought unprecedented challenges to the field of cybersecurity. As the volume of data and the sophistication of cyber threats grow, traditional approaches to securing systems and networks are no longer sufficient. In this context, artificial intelligence (AI) has emerged as a transformative force, offering advanced tools to detect, prevent, and respond to cyberattacks with greater efficiency and precision. The integration of AI technologies, particularly machine learning and deep learning, has opened new avenues for

developing scalable and adaptive cybersecurity solutions capable of addressing the evolving threat landscape.

This study adopts a comprehensive bibliometric approach to explore the state of research at the intersection of AI and cybersecurity. By analyzing a dataset of over 10,000 publications spanning 2022 to 2024, the study provides insights into the intellectual foundations, thematic trends, and collaborative dynamics that define this research ecosystem. Leveraging tools such as Biblioshiny [1], the analysis examines not only quantitative metrics, such as publication counts and citation impact, but also qualitative patterns, such as the relationships between core concepts and the emergence of new research directions. The analysis highlights the central role of machine learning as a driving force in cybersecurity research, with terms such as "data," "model," and "learning" recurring as focal points across abstracts, keywords, and titles. Through the construction of co-occurrence networks, the study reveals how these concepts are interconnected, forming distinct clusters that represent key areas of innovation, such as IoT security, privacy protection, and cloud resilience [2, 3, 4]. These findings underscore the interdisciplinary nature of the field, where advances in AI are closely linked to realworld applications and ethical considerations [5, 6]. Furthermore, the study examines the global distribution of research contributions, identifying leading countries, such as China, the United States, and India, as well as regions characterized by strong international collaboration, such as Europe and Australia. The role of influential journals and conferences, including ARXIV and IEEE ACCESS, is also explored, highlighting their importance in shaping the research agenda and disseminating highimpact work.

By combining thematic analysis with geographic and sourcebased insights, this study provides a holistic view of the research landscape in AI for cybersecurity [7, 8, 9]. The findings offer valuable perspectives for researchers, practitioners, and policymakers, emphasizing the need for continued innovation, collaboration, and ethical reflection in addressing the complex and everchanging challenges of the digital age.

2. Methods

2.1. Data collection

The data collection process for this bibliometric analysis was conducted systematically, leveraging the extensive capabilities of the Web of Science (WoS) Core Collection. This database was chosen for its robust indexing of peer-reviewed literature and its reputation for providing high-quality, multidisciplinary research outputs across scientific disciplines. The study utilized the Science Citation Index Expanded (SCI-EXPANDED), Social Sciences Citation Index (SSCI), and Emerging Sources Citation Index (ESCI) to ensure comprehensive coverage of relevant publications in the

domain of artificial intelligence and cybersecurity.

Construction of a clear and specific search string allows capturing the most wide-ranging types of research into topics touching on both aspects: AI and cybersecurity. In particular, using such a Boolean operation system allows for the maximization of the relevance-inclusiveness degree in the search output results: 'artificial intelligence' AND ('cybersecurity' OR 'machine learning' OR 'cloud computing' OR 'cyber attacks' OR 'security' OR 'privacy'). This query was designed to capture publications that discussed artificial intelligence in the context of cybersecurity and related topics, such as machine learning, cloud computing, and privacy. It ensured the inclusion of a wide range of studies addressing both technical advancements and practical applications in the field [10, 11, 12]. The query was applied across the entire WoS Core Collection, resulting in an initial dataset of 902,522 publications. These results spanned multiple disciplines, languages, document types, and years, reflecting the diverse and multidisciplinary nature of the topic. The decision to use Web of Science was driven by its comprehensive indexing and rigorous quality control, which ensured the inclusion of high-impact and peer-reviewed publications. The refinement strategy was carefully designed to balance inclusivity and specificity, ensuring that the dataset was both manageable and directly relevant to the research objectives.

Given the extensive scope of the initial dataset, a systematic refinement process was necessary to ensure that the final dataset was both manageable and directly relevant to the research objectives. The refinement process was informed by the PRISMA Statement (Preferred Reporting Items for Systematic Reviews and MetaAnalyses), a widely recognized evidence-based framework for documenting and reporting systematic reviews. While PRISMA was originally developed for systematic reviews in the healthcare domain, its principles were adapted in this study to enhance the transparency, rigor, and reproducibility of the bibliometric data selection process.

The refinement process involved the following steps:

1. Publications were restricted to those written in English, the predominant language of scientific communication. This decision was made to ensure consistency in the analysis and to facilitate the interpretation of publication metadata, abstracts, and keywords.

2. To focus on high-impact and peer-reviewed research outputs, only the following document types were included:

- Articles: Representing original research contributions;
- Review Articles: Summarizing and synthesizing current knowledge and trends;
- Proceedings Papers: Documenting emerging research presented at academic conferences;
- publications categorized as Retracted Publications or Data Papers were excluded to maintain the integrity of the dataset.

3. Only Open Access publications were included. This choice was driven by the principles of open science, ensuring that the selected publications were freely accessible to the broader research community and aligned with the goal of promoting transparency and reproducibility.

4. The dataset was limited to publications from the years 2022, 2023, and 2024. This three-year timeframe ensured a focus on the most recent research developments and trends in the field, aligning with the study's aim to provide insights into the latest advances.

5. To refine the dataset further, only publications indexed under specific Web of Science Categories were included. These categories were carefully chosen to align with the study's focus on artificial intelligence and cybersecurity and included:

- Communication;
- Computer Science Artificial Intelligence;
- Computer Science Cybernetics;
- Computer Science Hardware Architecture;
- Computer Science Information Systems;
- Computer Science Software Engineering Publications;
- unrelated categories, such as Agriculture Multidisciplinary or Chemistry Medicinal, were excluded to eliminate noise and enhance the relevance of the dataset.

After applying the refinement criteria, the dataset was reduced to 10,249 publications, distributed as follows:

- 2022: 3,226 publications.
- 2023: 3,465 publications.
- 2024: 3,558 publications.

The refined publication records were exported from WoS in plain text format. Due to limitations in the WoS platform, the export was conducted in batches of up to 500 records per file. These individual files were subsequently aggregated into a single compressed archive (ZIP format) to facilitate seamless import into Biblioshiny, an interactive interface of the Bibliometrix R package.

The final dataset represents a curated collection of high-quality publications that comprehensively cover recent advancements in artificial intelligence and cybersecurity. The dataset was prepared for bibliometric analysis by importing it into Biblioshiny, where descriptive metrics, science mapping, and visualization techniques were applied to uncover trends, collaborations, and thematic clusters in the field.

2.2. Analytical approach and data processing

Building upon the structured methodology described earlier, the Main Information Table

generated via Biblioshiny offers a distilled view of the dataset's key attributes, acting as a bridge between data collection and deeper analytical insights. While the earlier sections detailed the systematic approach used to refine and prepare the dataset, the Main Information Table provides a snapshot of the research landscape, highlighting essential metrics that define its scope, diversity, and collaborative dynamics.

Table 1. Main information's of the bibliometric analysis

DESCRIPTION	RESULTS
Main information about data	
Timespan	2022:2024
Sources (Journals, Books, etc.)	320
Documents	10249
Annual Growth Rate %	5.02
Average Citations per doc	6.001
References	418735
Authors	
Authors	30227
Authors of single-authored docs	588
Co-Authors per doc	4.09
International co-authorships %	33.64
Document types	
Article	9583
Proceedings paper	61
Review	605

By focusing on critical indicators such as the timespan, number of sources, document types, and authorship patterns, the table offers a foundational understanding of the field's structure and productivity. The dataset spans a three-year period from 2022 to 2024, reflecting the most recent advancements in the field. This temporal focus ensures that the analysis captures cutting-edge developments, emerging trends, and the current priorities of researchers addressing the intersection of AI and cybersecurity [13, 14]. The dataset encompasses publications from 320 distinct sources, including high-impact journals, conference proceedings, and other scholarly outlets. The diversity of sources indicates the interdisciplinary nature of the field, as AI-driven cybersecurity intersects with computer science, engineering, information systems, and related domains. This variety also suggests robust academic interest, with contributions distributed across specialized and generalist platforms. The 10,249 documents in the dataset are limited to articles, review articles, and proceeding papers, ensuring that the analysis focuses on peer-reviewed and rigorous academic contributions. This choice excludes less formal outputs like editorial notes or commentaries, enhancing the dataset's quality.

The mix of document types highlights both original research findings (articles) and

synthesized perspectives (review articles), alongside innovative ideas presented at conferences (proceeding papers). This combination is critical for understanding the field's foundations and identifying emerging research fronts. The dataset reflects a highly collaborative research environment, as evidenced by the number of contributing authors. The prevalence of multi-authored papers underscores the interdisciplinary and complex nature of the challenges addressed in AI for cybersecurity. Collaborative efforts likely span institutional, national, and even disciplinary boundaries, emphasizing the collective approach required to tackle global cybersecurity threats.

The inclusion of over 10,000 documents demonstrates not only the academic community's strong interest but also the practical importance of the topic. AI's role in combating cyber threats, enhancing data privacy, and ensuring secure computing environments has become a critical area of exploration, as evidenced by the breadth and diversity of the dataset.

3. Results

This section presents the findings of the bibliometric analysis, offering a comprehensive view of the research landscape in artificial intelligence (AI) applied to cybersecurity. By examining the dataset through descriptive metrics, science mapping, and thematic analysis, this study uncovers the key trends, intellectual foundations, and collaborative patterns that define the field. The results highlight both the breadth and depth of contributions, illustrating the dynamic evolution of research priorities and the interdisciplinary nature of this domain. The findings are structured to progressively build an understanding of the dataset, starting with an overview of scientific production trends, followed by an exploration of thematic clusters, and concluding with insights into global collaboration and influential research. This structured approach ensures a holistic perspective on the dataset, enabling the identification of critical areas for future exploration and collaboration.

3.1. Sources

The dataset extracted through Biblioshiny highlights the top 10 sources contributing to the research landscape in artificial intelligence (AI) applied to cybersecurity. These sources are ranked based on the number of articles published, reflecting their significance in disseminating knowledge and advancing the field.

Table 2. 10 most relevant sources of the dataset

Sources	Articles
INFORMATION	660

JOURNAL OF KING SAUD UNIVERSITY-COMPUTER AND INFORMATION SCIENCES	561
FUTURE INTERNET	504
COMPUTERS & SECURITY	370
JOURNAL OF CLOUD COMPUTING-ADVANCES SYSTEMS AND APPLICATIONS	315
FRONTIERS IN ARTIFICIAL INTELLIGENCE	280
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	231
ARTIFICIAL INTELLIGENCE REVIEW	212
COMPLEX & INTELLIGENT SYSTEMS	208
SCALABLE COMPUTING-PRACTICE AND EXPERIENCE	205

Leading the dataset is “Information”, with the highest number of publications, indicating its role as a central hub for disseminating research that spans foundational AI methodologies and their practical applications in cybersecurity. Following closely, journals like the “Journal of King Saud University-Computer and Information Sciences” and “Future Internet” reflect the growing interest in AI's role within internet technologies and digital ecosystems, emphasizing their interdisciplinary appeal [15, 16]. Specialized outlets such as “Computers & Security” and “IEEE Transactions on Dependable and Secure Computing” focus more narrowly on topics directly addressing cybersecurity challenges. These journals provide platforms for rigorous explorations into intrusion detection systems, privacy-preserving algorithms, and the resilience of AI-enhanced security frame-works. Their prominence underscores the importance of deep technical insights in advancing the field. Furthermore, journals like the “Journal of Cloud Computing” and “IEEE Internet of Things Journal” highlight emerging areas of interest, particularly the intersection of AI with cloud architectures and IoT security. These contributions reflect the shifting priorities of researchers as they tackle vulnerabilities introduced by increasingly connected systems and the reliance on distributed computing environments. In addition to these specialized sources, interdisciplinary journals such as “Frontiers in Artificial Intelligence” and “Complex & Intelligent Systems” indicate the field's breadth, incorporating perspectives from complexity theory, intelligent systems design, and adaptive security measures. These publications bridge traditional AI research with practical applications in secure environments, revealing innovative approaches to addressing cyber threats. Overall, the dataset showcases a well-balanced representation of foundational research, application-driven studies, and emerging trends. The presence of both specialized and interdisciplinary journals underlines the necessity of a collaborative and multifaceted approach to advancing AI in cybersecurity, as researchers continue to address increasingly complex and global challenges. These findings provide a strong basis for analyzing thematic trends and collaborative dynamics in subsequent sections.

Building on the analysis of the most relevant sources, which highlighted the outlets contributing the highest number of publications to the research landscape, it is equally important to examine the impact of these and other sources in terms of citations. While publication volume reflects the breadth of research dissemination, citation counts provide a deeper understanding of the intellectual influence and recognition within the scholarly community. The focus now shifts to the most cited sources, which represent the foundational and high-impact publications shaping the field of artificial intelligence for cybersecurity. These sources highlight the key venues through which groundbreaking ideas, methodologies, and applications have resonated across the research community, offering a complementary perspective to the publication trends previously discussed.

Table 3. 10 most cited sources of the dataset

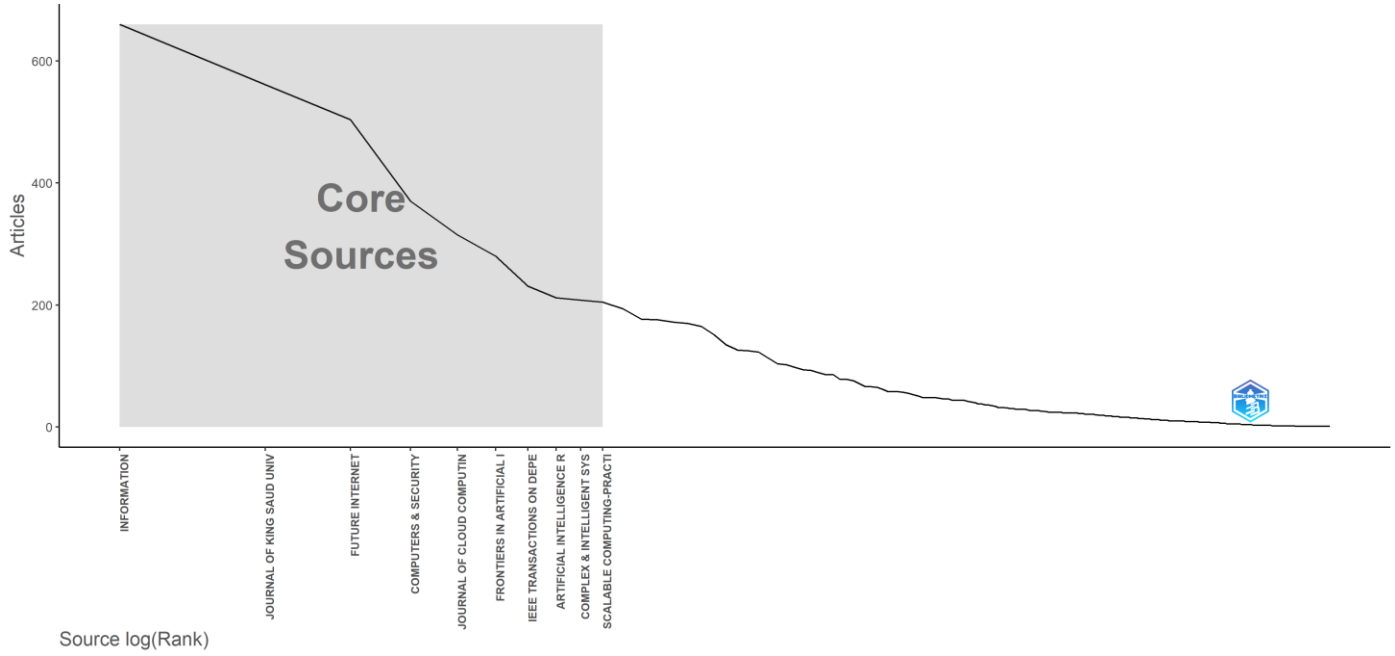
Sources	Articles
ARXIV	19916
LECT NOTES COMPUT SC	11318
IEEE ACCESS	10526
PROC CVPR IEEE	6081
ADV NEUR IN	4652
IEEE INTERNET THINGS	3770
SENSORS-BASEL	3626
PR MACH LEARN RES	3408
EXPERT SYST APPL	3278
COMPUT SECUR	2698

The dataset reveals a rich landscape of citation activity, highlighting key sources that have had a significant influence on research in artificial intelligence (AI) applied to cyber-security. These sources span preprint platforms, journals, and conference proceedings, reflecting the diversity of channels through which foundational and applied knowledge is disseminated in this field. Leading the list is ARXIV, with an impressive 19,916 citations, emphasizing its pivotal role in facilitating the rapid dissemination of cutting-edge research. As a preprint repository, ARXIV is widely recognized for hosting early-stage work in AI, including foundational methodologies and innovative applications in cybersecurity [26]. Similarly, LECT NOTES COMPUT SC, with 11,318 citations, underscores the influence of conference proceedings, which are vital for presenting novel ideas and engaging the academic community. Journals such as IEEE ACCESS and ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS (ADV NEUR IN) have garnered 10,526 and 4,652 citations, respectively. These publications reflect the integration of theoretical AI advancements with practical applications in cybersecurity. IEEE ACCESS, in particular, is known for its multidisciplinary approach and rapid publication process, making it a preferred venue for impactful

research. Publications like IEEE INTERNET OF THINGS JOURNAL (3,770 citations) and SENSORS-BASEL (3,626 citations) highlight the increasing focus on securing IoT ecosystems and sensor-based technologies. These sources emphasize the application of AI to address vulnerabilities in highly connected and data-driven environments, showcasing the evolving priorities in cybersecurity research. COMPUTERS & SECURITY, a journal already identified as one of the most prolific sources, continues to demonstrate its influence with 2,698 citations. Its presence in both publication and citation rankings reinforces its critical role in advancing knowledge on intrusion detection, encryption methods, and AI-driven threat mitigation. The high citation counts of PROC CVPR IEEE (6,081 citations) and PR MACH LEARN RES (3,408 citations) reflect the importance of conferences in shaping the research agenda. These venues are particularly influential in domains like computer vision and machine learning, where new techniques are rapidly applied to cybersecurity challenges.

The citation activity in this dataset reflects the dynamic and interdisciplinary nature of research in AI for cybersecurity. The dominance of ARXIV and conference proceedings highlights the field's reliance on rapid dissemination platforms to keep pace with technological advancements. At the same time, the presence of specialized journals underscores the need for in-depth explorations of targeted topics, from IoT security to neural network reliability. This citation landscape not only underscores the diverse sources of influence in the field but also sets the stage for exploring how these sources contribute to thematic trends and intellectual structures in subsequent analyses [27, 28]. Following the exploration of the most cited sources, which provided insights into the intellectual impact and foundational venues shaping the field of artificial intelligence (AI) for cybersecurity, it is crucial to examine how these sources are distributed and their relative importance in disseminating research. Bradford's Law offers a systematic framework for understanding this distribution, revealing how scholarly publications are concentrated across a few core journals while others contribute less frequently but still provide value [17, 18, 19]. Bradford's Law, introduced by Samuel C. Bradford in 1934, states that a small number of journals (the "core zone") produce the majority of articles on a particular topic, while the remaining journals contribute fewer publications, distributed across progressively larger groups or zones. This principle is instrumental in bibliometric analysis, as it identifies the most productive sources and highlights the core journals essential for comprehensive research coverage. The application of Bradford's Law to the dataset provides a structured view of how knowledge in AI and cybersecurity is disseminated, complementing the citation analysis by focusing on productivity and the distribution of research outputs. Below, we analyze the data to uncover the field's core, intermediate, and peripheral journals.

Figure 1. Core sources by Bradford's Law



According to Bradford's Law, the core sources—classified as Zone 1—represent the most productive journals and platforms in the field, responsible for a disproportionately high share of publications. In this dataset, 10 core sources contribute a total of 3,546 articles, highlighting their central role in disseminating research on artificial intelligence (AI) applied to cybersecurity. The core sources include prominent outlets such as INFORMATION, JOURNAL OF KING SAUD UNIVERSITY-COMPUTER AND INFORMATION SCIENCES, and FUTURE INTERNET, which have already been identified as top contributors in terms of both publication volume and influence. These journals provide a concentrated body of knowledge, making them essential for researchers seeking comprehensive coverage of the field's developments. The identification of these core sources aligns with Bradford's principle that a small number of sources account for the majority of significant publications. Their inclusion in Zone 1 emphasizes their pivotal role in shaping the research landscape and highlights them as indispensable resources for future investigations.

After identifying the core sources central to the field through Bradford's Law, it is important to delve deeper into their local impact within the research landscape. While publication volume and core categorization highlight productivity, metrics such as the h-index, g-index, and citation counts provide a nuanced understanding of a source's quality, influence, and enduring relevance [20, 21, 22]. These indicators measure the local impact of sources, capturing their ability to drive forward the research conversation in artificial intelligence (AI) and cybersecurity.

Table 4. Top 10 sources' local impact by their index score

Source	H_index	G_index	M_index	TC	NP
JOURNAL OF KING SAUD UNIVERSITY-COMPUTER AND INFORMATION SCIENCES	37	54	9.250	6558	561
ARTIFICIAL INTELLIGENCE REVIEW	26	54	6.500	3234	212
COMPLEX & INTELLIGENT SYSTEMS	26	38	6.500	2231	208
KNOWLEDGE-BASED SYSTEMS	25	37	6.250	1864	170
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	24	39	6.000	2330	231
NEUROCOMPUTING	24	27	6.000	1893	177
NEURAL COMPUTING & APPLICATIONS	22	35	5.500	2172	194
COMPUTERS & SECURITY	21	29	5.250	2407	370
FUTURE INTERNET	20	29	5.000	2314	504
IEEE TRANSACTIONS ON SERVICES COMPUTING	20	34	5.000	1499	125

The dataset on source impact provides key bibliometric indicators for each source:

- h-index: Reflects the number of articles (h) that have received at least h citations, indicating consistent productivity and citation impact.
- g-index: Highlights the influence of highly cited articles, complementing the h-index by giving additional weight to the most impactful works.
- m-index: Measures the h-index normalized by the years since the first publication, providing insight into the source's citation trajectory.
- TC (Total Citations): Captures the cumulative citation count of a source's publications.
- NP (Number of Publications): Represents the total number of articles published by the source.
- PY_start: Indicates the starting year of the source's contributions to the dataset.

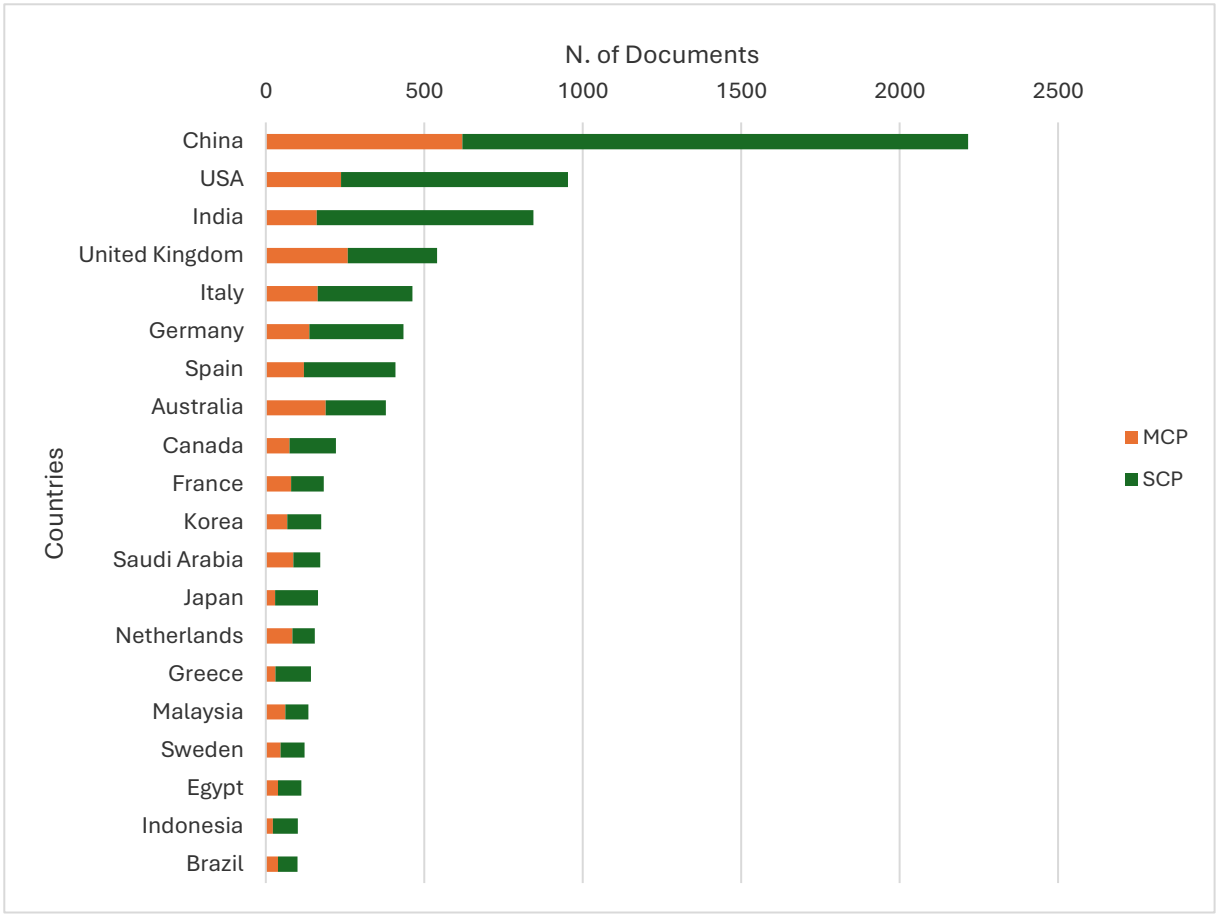
The local impact of sources within the field of artificial intelligence (AI) applied to cybersecurity reveals significant insights into their scholarly influence, productivity, and consistency. Among the leading contributors, the Journal of King Saud University-Computer and Information Sciences stands out with the highest h-index (37) and g-index (54), supported by a substantial 6,558 citations across 561 publications. These metrics underline its central role in disseminating widely recognized and impactful research. Similarly, the Artificial Intelligence Review demonstrates notable influence with an h-index of 26, a matching g-index of 54, and 3,234 citations, reflecting its

emphasis on synthesizing critical advancements in the field. Other key sources, such as Complex & Intelligent Systems and Knowledge-Based Systems, show balanced performance, with h-indices of 26 and 25, respectively. Their contributions reflect a strong focus on methodologies and AI-driven solutions relevant to cybersecurity. IEEE journals also feature prominently, with IEEE Transactions on Dependable and Secure Computing achieving an h-index of 24, highlighting its role in advancing secure and robust computing systems. The m-index, which normalizes the h-index over time, highlights the exceptional trajectory of the Journal of King Saud University with a score of 9.25, far exceeding its peers. This indicates a rapid and significant impact in a relatively short span, reaffirming its importance in the field. Other sources, such as the Artificial Intelligence Review and Complex & Intelligent Systems, also maintain steady and impactful citation patterns, with m-indices of 6.5 each. In terms of cumulative citations, sources like Computers & Security and Future Internet continue to exhibit strong practical relevance despite slightly lower h-indices, emphasizing the importance of applied research in shaping the field. These findings underscore the complementary roles of productivity and citation impact in advancing the domain, with each source contributing uniquely to the evolving discourse in AI and cybersecurity.

3.2. Authors

Having established the influence and productivity of individual sources, the focus now shifts to the geographical distribution of research efforts. Understanding the contributions of different countries provides critical insights into the global dynamics of research collaboration and production in AI applied to cybersecurity. The analysis begins with the role of corresponding authors, followed by an overview of the total scientific production for the top 20 countries.

Figure 2. Corresponding author's countries sorted by MCP's (multiple-country publications) and SCP's (single-country publications)

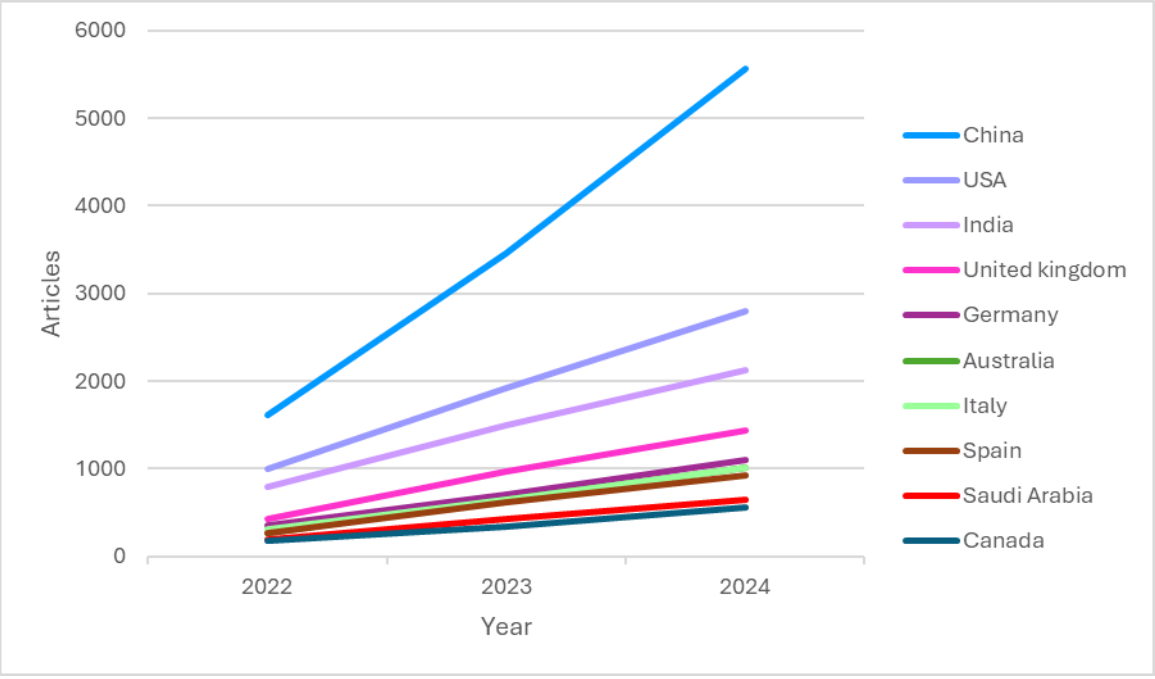


The dataset reveals the distribution of research contributions among countries, emphasizing both the volume of publications and the degree of international collaboration. China stands out as the most prolific contributor, with 2,216 articles representing 21.6% of the total publications. A significant portion of this output, amounting to 1,596 articles, is classified as single-country publications (SCP), reflecting a strong domestic research base. However, China's multiple-country publications (MCP) account for 28% of its total output, indicating a relatively lower level of international collaboration compared to other major contributors. The United States follows with 953 articles, constituting 9.3% of the dataset. Of these, 716 are SCP and 237 MCP, with an MCP percentage of 24.9%. This balance underscores the United States' capacity for both independent research and international partnerships. India ranks third with 844 articles, representing 8.2% of the total, and while the majority are SCP, its MCP percentage is lower at 19.1%, reflecting a predominantly domestic focus in its research efforts. European countries such as the United

Kingdom, Italy, and Germany have contributed in volume and collaboration aspects. The United Kingdom, with 540 articles (5.3%), is distinguished by an MCP of 47.8%, depicting its robust engagement with international research networks. Similarly, Italy and Germany contribute with 463 and 434 articles, respectively, with a balanced approach: 35.4% and 31.6% MCP, showing significant cross-border collaborations. Australia comes out to be an important player with 379 articles and a very high MCP percentage of 49.9%, reflecting its strategic dependence on and contribution to international collaboration. Other countries, such as France and Canada, have smaller total outputs of 183 and 221 articles, respectively, but their collaboration rates are high, with MCP percentages of 43.7% and 33.9%, respectively, underlining their positions as active players in global research networks. This analysis also points out different strategies that different countries have been following to promote research in AI and cybersecurity: while some stress heavily on domestic production, others focus on international collaboration, so that the research landscape becomes globally interconnected and fosters innovation in tackling common challenges related to cybersecurity.

The temporal comparison of countries' scientific production shows in detail how the contribution of research into artificial intelligence and cybersecurity has changed over time. It would be possible to underline a different growth profile among leading nations, together with changes in the focus of their research interests.

Figure 3. Top 10 countries articles production over time

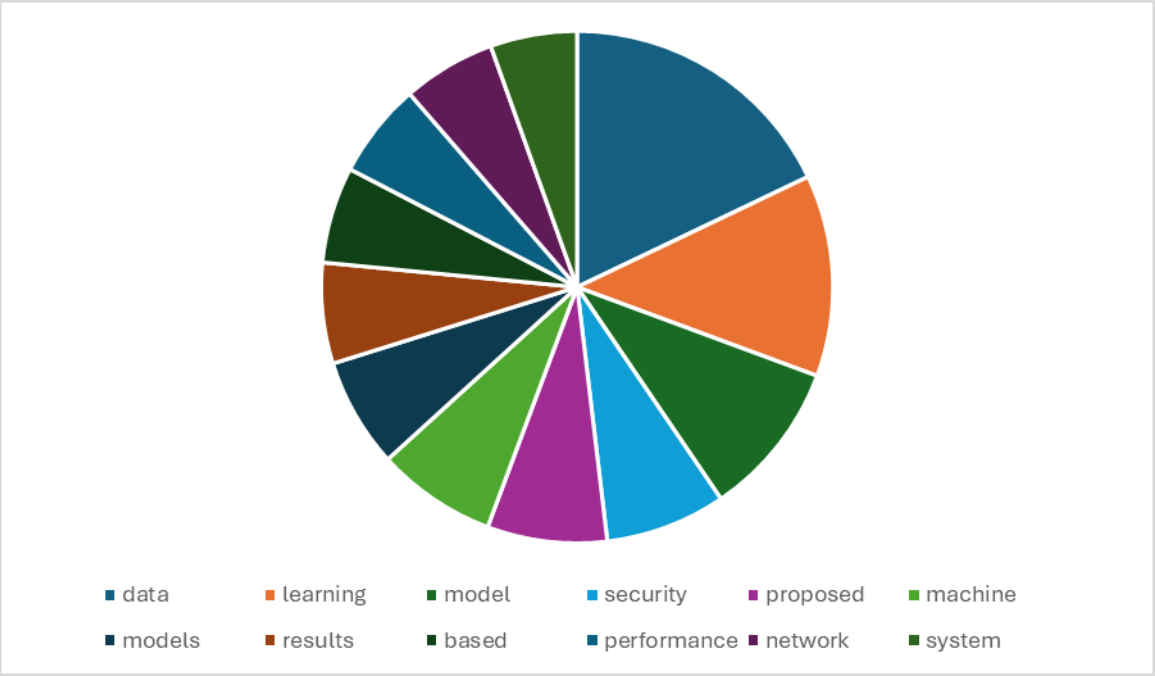


China leads with an impressive total of 5,566 publications, reflecting its sustained and significant investment in AI-driven cybersecurity research. This dominance suggests a strong commitment to developing and disseminating innovations, supported by its rapidly expanding academic and industrial research infrastructure [23, 24]. The United States follows with 2,800 publications, maintaining its historical leadership in the field. The steady output from the United States reflects its established research ecosystem and ongoing advancements in both theoretical and applied AI for cybersecurity [29]. India, with 2,128 publications, has emerged as a major contributor, reflecting the country's increasing focus on technological innovation and its strategic investments in AI and cyber-security. The United Kingdom and Germany contribute 1,440 and 1,098 publications respectively, underscoring their roles as European leaders in the domain. Both nations show consistent output, supported by robust academic institutions and international collaborations. Australia, Italy, and Spain also demonstrate significant contributions, with outputs of 1,017, 1,008, and 922 publications respectively. These countries, while smaller in total output compared to China or the United States, exhibit strong growth trajectories, indicating their rising influence in the global research landscape. Saudi Arabia, with 653 publications, represents a growing player in the field, reflecting its strategic focus on developing AI capabilities and cybersecurity frameworks. The trends in scientific production over time highlight the dynamic nature of research in AI and cybersecurity. While traditional powerhouses like the United States and the United Kingdom maintain their influence, emerging contributors such as India and Saudi Arabia reflect the globalization of research efforts. This temporal analysis emphasizes the importance of understanding regional strengths and collaborative opportunities in addressing the shared challenges posed by cybersecurity threats in an increasingly digital world.

3.3. Words and Topics

Building on the geographical analysis of scientific production, which highlighted the global distribution of research efforts in artificial intelligence (AI) for cybersecurity, we now shift focus to the thematic core of this research field. By examining the most frequent words used in article abstracts, we gain valuable insights into the key concepts, methodologies, and priorities shaping the scholarly discourse. Abstracts serve as concise summaries of research contributions, and their language reveals the dominant trends and recurring themes within the dataset.

Figure 4. Most frequent words in abstracts of the analyzed documents



The analysis of word frequencies underscores the central themes of research in AI and cybersecurity. The term "data", appearing 15,786 times, emerges as the most prominent, reflecting its foundational role in this domain. Whether discussing secure data management, data-driven AI models, or the protection of sensitive information, the concept of data permeates much of the research activity. Closely tied to this is the term "learning", which appears 11,221 times. Its prevalence points to the critical role of machine learning and deep learning approaches in addressing complex cybersecurity challenges, from anomaly detection to predictive threat analysis. Another frequently used term is "model", occurring 8,694 times, emphasizing the importance of developing computational frameworks for tasks such as intrusion detection and risk assessment. The iterative process of proposing, refining, and testing these models is central to advancing both theoretical and applied aspects of the field. This aligns with the frequent use of the word "proposed", which appears 6,680 times, highlighting the exploratory and innovative nature of the research. The term "security", with 6,713 occurrences, reinforces the primary focus on safeguarding systems and networks. Whether discussing encryption, authentication mechanisms, or AI-driven threat mitigation, security remains at the heart of the discourse. Similarly, terms like "performance" (5,299 occurrences) and "results" (5,614 occurrences) reflect the emphasis on empirical validation and evaluation of AI

frameworks, ensuring that proposed methodologies are effective, efficient, and scalable in real-world scenarios. The frequent use of "machine" (6,671 occurrences) alongside "learning" emphasizes the reliance on AI technologies for automating and enhancing cybersecurity efforts. The methodological aspect of the research is further highlighted by the word "based" (5,356 occurrences), often used in contexts such as "data-based" or "model-based" approaches, underscoring the reliance on structured and data-driven methodologies.

This lexical analysis reveals a research landscape deeply entrenched in data-centric methodologies, iterative model development, and security-driven applications. The frequent mention of "proposed" and "results" indicates a strong focus on empirical research and innovation, while terms like "learning" and "machine" highlight the central role of AI technologies in addressing cybersecurity challenges. These findings provide a thematic snapshot of the research priorities and methodologies dominating the field, offering a foundation for exploring deeper trends and connections between topics in subsequent analyses. The consistent presence of key terms underscores the alignment of the research focus with the evolving demands of cybersecurity in an increasingly data-driven world.

Following the examination of the most frequent words in abstracts, which offered a thematic overview of the language used in summarizing research, we now delve into the analysis of keywords. Keywords, selected explicitly by authors, serve as concise representations of a paper's core focus and methodologies. They offer a direct glimpse into the research priorities and topics driving the field, complementing the insights gained from abstract analysis.

Figure 5. Most frequent words in keywords of the analyzed documents

The keyword analysis reveals the recurring themes and concepts that define the research

landscape in artificial intelligence (AI) and cybersecurity. At the forefront is "internet", appearing 437 times, highlighting its integral role in discussions around network security, IoT (Internet of Things), and cyber threats in highly connected environments. The term "model", with 433 occurrences, reflects the emphasis on developing and refining computational frameworks to address cybersecurity challenges. Models, particularly AI-driven ones, form the backbone of predictive and preventative strategies in this field. "Classification", used 416 times, underscores the widespread application of machine learning techniques for categorizing threats, analyzing behaviors, and detecting anomalies. Similarly, "security", appearing 320 times, continues to affirm its foundational presence, aligning with the broader theme of safeguarding systems and networks. The term "framework" (311 occurrences) points to the development of comprehensive systems and methodologies that integrate multiple technologies for robust cybersecurity solutions. Other prominent keywords include "algorithm" (281 occurrences), highlighting the role of computational processes in optimizing threat detection and mitigation strategies, and "system" (271 occurrences), reflecting discussions around building secure, efficient infrastructures. The appearance of "prediction" (231 occurrences) signals the increasing reliance on predictive analytics for proactive cybersecurity measures, while "privacy" (221 occurrences) emphasizes concerns around safeguarding sensitive data in an interconnected world. Finally, "networks" (214 occurrences) reflects the focus on securing networked systems, from corporate infrastructures to IoT ecosystems.

Following the analysis of keywords, which provided insights into the core themes and concepts driving the research, the focus now shifts to the most frequently used words in publication titles. Titles, as succinct summaries of research contributions, highlight the primary focus and methodologies of individual studies, offering a direct window into the research priorities within the field.

Figure 6. TreeMap of the most frequent words in titles of the analyzed documents

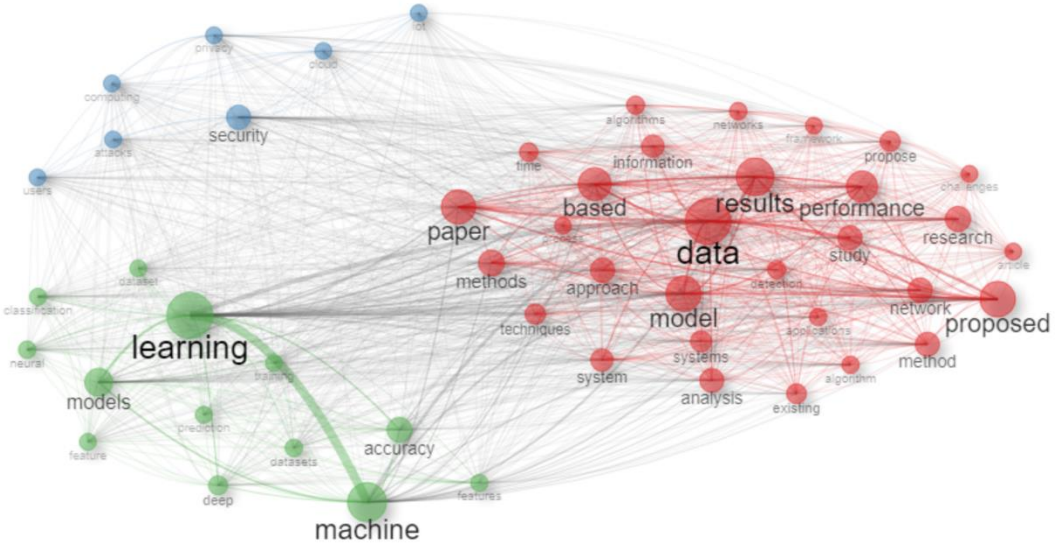
The term "learning", appearing 2,365 times, is the most frequently used word in publication titles, underscoring the dominance of machine learning and related methodologies in addressing cybersecurity challenges. Closely tied to this is "machine", with 1,274 occurrences, further emphasizing the centrality of machine learning in this domain. The word "based", appearing 1,164 times, reflects the methodological focus on data-based and model-based approaches, which are prevalent in AI-driven research. "Data" (1,153 occurrences) and "detection" (1,004 occurrences) highlight the importance of analyzing and securing data as well as the critical role of detection systems, such as intrusion detection and anomaly detection, in cybersecurity. Words like "deep" (741 occurrences) and "analysis" (691 occurrences) indicate the reliance on deep learning techniques and comprehensive analyses to address complex problems. "Security" (609 occurrences), along with "model" (606 occurrences) and "network" (591 occurrences), reinforces the alignment of research efforts with the overarching goal of securing digital environments and developing robust computational models.

The frequent appearance of these terms reflects a strong emphasis on machine learning, deep learning, and data-driven approaches in AI applied to cybersecurity. The focus on detection systems, security frameworks, and network protection highlights the field's commitment to addressing practical challenges, aligning closely with the theme of advancing AI methodologies to safeguard digital ecosystems [25]. These findings further contextualize the thematic trends and methodological priorities identified in the abstract and keyword analyses.

4. Discussion

We revealed a dynamic and interconnected research landscape where artificial intelligence (AI) plays a pivotal role in addressing modern cybersecurity challenges. By examining abstracts, keywords, and titles, the study has highlighted key thematic priorities and trends. To further deepen our understanding of the intellectual structure and relationships within the field, we went further and analyzed the co-occurrence network of abstracts, which provides critical insights into how terms and concepts interrelate, offering a roadmap of the research ecosystem.

Figure 7. Co-occurrence network of the frequent words used in abstracts of the analyzed documents



The co-occurrence network of abstracts illustrates the relationships and connections between frequently used terms, reflecting how the research field is organized around key themes and methodologies. Terms like "learning" and "data" emerge as central nodes in the network, with the highest PageRank values, signifying their foundational importance in AI and cybersecurity research. The network clusters these terms into distinct thematic groups, each representing a significant area of focus within the field.

One prominent cluster revolves around "learning," "machine," and "models," highlighting the critical role of machine learning and related methodologies. This cluster emphasizes advancements in neural networks, classification techniques, and predictive analytics, which are essential for developing robust intrusion detection systems and other cybersecurity tools. The prominence of these terms reflects the research community's reliance on AI-driven solutions to address evolving threats.
Another key cluster focuses on "data," "model," and "results," representing the iterative process of designing, testing, and refining computational frameworks. The emphasis on "data" highlights its dual role as both an asset for training AI models and a vulnerability requiring protection. Terms like "results" and "performance" within this cluster underline the importance of evaluating the efficacy and scalability of proposed solutions, ensuring they are both practical and reliable.

The third cluster is anchored by terms like "security," "privacy," and "cloud," signaling a growing focus on applied research areas. This cluster reflects efforts to secure interconnected systems, protect sensitive information, and address vulnerabilities in cloud computing and IoT infrastructures. The inclusion of "privacy" in this cluster emphasizes the ethical considerations associated with AI-driven cybersecurity, particularly in safeguarding user data and maintaining trust.

The network’s structure reveals an intricate interplay between foundational and application-driven research. Clusters centered around "learning" and "data" highlight the theoretical advancements that enable practical implementations, while the "security" and "privacy" cluster underscores the pressing need for solutions tailored to real-world challenges. The interconnectedness of these clusters demonstrates the interdisciplinary nature of the field, requiring collaboration across computer science, engineering, ethics, and policy domains. This analysis also points to emerging priorities such as securing IoT environments and addressing privacy concerns, which align with broader technological trends. The high betweenness centrality of terms like "learning" and "security" underscores their role as bridges between different research areas, facilitating the integration of AI methodologies into practical cybersecurity applications.

The findings of this bibliometric analysis provide a comprehensive understanding of the evolving research landscape in artificial intelligence (AI) applied to cybersecurity. By combining systematic data collection, descriptive analysis, and thematic exploration, the study highlights key advancements, intellectual foundations, and collaborative patterns that shape this rapidly growing interdisciplinary domain. AI technologies are revolutionizing the field of cybersecurity by addressing the increasing complexity of threats in highly connected and data-driven environments. The analysis reveals that research efforts are strongly rooted in data-centric methodologies, with terms like "data," "learning," and "model" dominating abstracts, keywords, and titles. These terms are underlined by the critical role of machine learning and deep learning in the detection of anomalies, the prediction of

threats, and security regarding digital ecosystems. The emphasis on "security" and "detection" also shows the core mission of the field: protection of systems and networks from cyberattacks.

The geographical analysis of the research contributions reveals that this domain is highly global, with China, the United States, and India emerging as leading knowledge producers. However, the data also indicate a mismatch in international collaboration, with countries such as the United Kingdom, Australia, and France showing higher levels of cross-border partnerships. This is very important in global collaboration on cybersecurity challenges, which are intrinsically transnational and require coordination at multiple levels to effectively minimize risks.

Citation and productivity metrics denote a core-dependent field, with a core set of sources drawing heavily upon highly influential publications. Such platforms as ARXIV, IEEE ACCESS, and COMPUTERS & SECURITY are considered keystones for foundational and applied knowledge dissemination, as Bradford's Law will bear out. High-impact journals and high-impact conferences reflect the dynamic and interdisciplinary nature of this research environment.

Some of the emergent trends, such as "privacy," "IoT," and "framework," denote the rise of interest in security issues regarding the connected environment and ethical problems. In general, this integration of AI into cloud computing, IoT infrastructures, and mechanisms of privacy preservation demonstrate how the area adapts to new technological challenges and stays oriented toward practical applications.

Overall, the analysis reveals a balanced representation of foundational research, application-driven studies, and collaborative efforts. This combination is essential for advancing the field and ensuring that AI technologies remain effective and ethical tools in the fight against cybersecurity threats. Future research should continue to explore these intersections, fostering innovation while addressing the multifaceted risks posed by an increasingly digital world.

5. Conclusions

AI is playing a crucial role in cybersecurity because it actively detects, prevents, and manages a number of highly connected, complex cyber-attacks. The bibliometric review carried out on more than 10,000 publications from the period 2022 to 2024 marks points in data-driven approaches by putting machine learning at the core of deep learning. Key research themes include predictive analytics, anomaly detection, and protection of IoT and cloud infrastructures, with an emphasis on the important role AI plays in protecting digital ecosystems. Looking across the geographical distribution of research production, China, the United States, and India lead, though countries like the United Kingdom and Australia are leaders in terms of international collaboration, which is crucial for solving global cybersecurity challenges. Influential sources are ARXIV, IEEE ACCESS, and

COMPUTERS & SECURITY, which combine theoretical and practical advances at the leading edges, underpinning the research landscape. The growing trends are security in IoT, privacy protection, and ethical AI deployment, hence showing the area of adaptability to emerging technological challenges. In contrast, the result underlines only AI-driven cybersecurity research that will be increasingly multidisciplinary, collaborative, inventive, and especially ethical, needing global partnerships trying to keep up with an evolving threat landscape.

6. Bibliographic References

[1] Aria, M. & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis, Journal of Informetrics, 11(4), pp 959-975, Elsevier, DOI: 10.1016/j.joi.2017.08.007.

[2] Ganji, K. and Afshan, N. (2024), "A bibliometric review of Internet of Things (IoT) on cybersecurity issues", Journal of Science and Technology Policy Management, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSTPM-05-2023-0071.

[3] Flores-Cerrillo J, He QP, Wang J and Yu H (2023) Editorial: Smart manufacturing: advances and applications of artificial intelligence, machine learning and industrial internet of things in the chemical and biochemical industry. Front. Chem. Eng. 5:1309165. doi: 10.3389/fceng.2023.1309165.

[4] S. Girish Savadatti, K. Srinivasan and Y. -C. Hu, "A Bibliometric Analysis of Agent-Based Systems in Cybersecurity and Broader Security Domains: Trends and Insights," in IEEE Access, vol. 13, pp. 90-119, 2025, doi: 10.1109/ACCESS.2024.3520583.

[5] Fraile-Rojas, B., De-Pablos-Heredero, C. and Mendez-Suarez, M. (2025), "Female perspectives on algorithmic bias: implications for AI researchers and practitioners", Management Decision, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/MD-04-2024-0884.

[6] Jačisko, Jakub MD, PhD; Veselý, Viktor MD; Chang, Ke-Vin MD, PhD; Özçakar, Levent MD. (How) ChatGPT—Artificial Intelligence Thinks It Can Help/Harm Physiatry. American Journal of Physical Medicine & Rehabilitation 103(4):p 346-349, April 2024. | DOI: 10.1097/PHM.0000000000002370.

[7] Orosco-Fabian, J. R. (2024). Cybersecurity in higher education: a bibliometric review. Revista Digital De Investigación En Docencia Universitaria, 18(2), e1933. https://doi.org/10.19083/ridu.2024.1933.

[8] Yu, H. et al. (2023) 'Literature review on maritime cybersecurity: state-of-the-art', Journal of Navigation, 76(4–5), pp. 453–466. doi:10.1017/S0373463323000164..

[9] Deepak Sharma, Ruchi Mittal, Ravi Sekhar, Pritesh Shah, Matthias Renz, A bibliometric analysis of cyber security and cyber forensics research, Results in Control and Optimization, Volume 10, 2023, 100204, ISSN 2666-7207, https://doi.org/10.1016/j.rico.2023.100204.

[10] Abawajy, J. (2012). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787.

[11] Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N.; Capretz, L.F.; Abdulkadir, S.J. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics 2022, 11, 198. https://doi.org/10.3390/electronics11020198.

[12] Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology. 2020; 71: 939–953. https://doi.org/10.1002/asi.24311.

[13] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[14] Alves, J.; Lima, T.M.; Gaspar, P.D. Is Industry 5.0 a Human-Centred Approach? A Systematic Review. Processes 2023, 11, 193. https://doi.org/10.3390/pr11010193.

[15] Laux, J. Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act. AI & Soc 39, 2853–2866 (2024). https://doi.org/10.1007/s00146-023-01777-z.

[16] B. S. Coventry and E. L. Bartlett, "Closed-Loop Reinforcement Learning Based Deep Brain Stimulation Using SpikerNet: A Computational Model," 2023 11th International IEEE/EMBS Conference on Neural Engineering (NER), Baltimore, MD, USA, 2023, pp. 1-4, doi: 10.1109/NER52421.2023.10123797.

[17] VICKERY, B.C. (1948), "BRADFORD'S LAW OF SCATTERING", Journal of Documentation, Vol. 4 No. 3, pp. 198-203. https://doi.org/10.1108/eb026133.

[18] NARANAN, S. Bradford's Law of Bibliography of Science: an Interpretation. Nature 227, 631–632 (1970). https://doi.org/10.1038/227631a0.
[19] Rubén Urbizagástegui Alvarado, Growth of Literature on Bradford's Law, Investigación Bibliotecológica: Archivonomía, ibliotecología e Información, Volume 30, Issue 68, Supplement, 2016, Pages 51-72, ISSN 0187-358X, https://doi.org/10.1016/j.ibbai.2016.06.003.
[20] Ahmad, S. A. J., Abdel-Magid, I. M., & Hussain, A. (2017). Comparison among journal impact factor, SCimago journal rank indicator, eigenfactor score and h5-index of environmental engineering journals. COLLNET Journal of Scientometrics and Information Management, 11(1), 133–151. https://doi.org/10.1080/09737766.2016.1266807.
[21] Anderson, T., Hankin, R., & Killworth, P. (2008). Beyond the Durfee square: Enhancing the h-index to score total publication output. Scientometrics, 76(3), 577-588. https://doi.org/10.1007/s11192-007-2071-2.
[22] Roldan-Valadez, E., Salazar-Ruiz, S.Y., Ibarra-Contreras, R. et al. Current concepts on bibliometrics: a brief review about impact factor, Eigenfactor score, CiteScore, SCImago Journal Rank, Source-Normalised Impact per Paper, H-index, and alternative metrics. Ir J Med Sci 188, 939–951 (2019). https://doi.org/10.1007/s11845-018-1936-5.
[23] Luo, Xibeili, Exploring the Role of Mindfulness-Based Interventions in Enhancing Psychological Capital and Academic Adjustment among Chinese Students, American Journal of Health Behavior, Volume 48, Number 5, October 2024, pp. 1332-1345(14), https://doi.org/10.5993/AJHB.48.5.13.
[24] Carver, J. (2024). Developing digital “peripheries" for strategic advantage: Capacity building assistance and strategic competition in Africa. Contemporary Security Policy, 1–42. https://doi.org/10.1080/13523260.2024.2430021.
[25] Aiyanyo, I.D.; Samuel, H.; Lim, H. A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. Appl. Sci. 2020, 10, 5811. https://doi.org/10.3390/app10175811.
[26] Colin B. Clement, Matthew Bierbaum, Kevin P. O'Keeffe, Alexander A. Alemi, On the Use of ArXiv as a Dataset, ICLR 2019, arXiv:1905.00075, https://doi.org/10.48550/arXiv.1905.00075.
[27] Davis, P.M., Fromerth, M.J. Does the arXiv lead to higher citations and reduced publisher downloads for mathematics articles?. Scientometrics 71, 203–215 (2007). https://doi.org/10.1007/s11192-007-1661-8.
[28] Haque, A.-u. and Ginsparg, P. (2009), Positional effects on citation and readership in arXiv. J. Am. Soc. Inf. Sci., 60: 2203-2218. https://doi.org/10.1002/asi.21166.
[29] Sandoval Bravo, M.P. (2024) ‘Carlos Solar, Cybersecurity Governance in Latin America: States, Threats, and Alliances State University of New York Press, 2023, pp. 352’, Journal of Latin American Studies, 56(1), pp. 170–172. doi:10.1017/S0022216X24000221.