Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 158-169
DOI: https://doi.org/10.58496/MJCS/2023/018; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Cybersecurity and Artificial Intelligence Applications: A Bibliometric Analysis Based on Scopus Database

O. S. Albahri [1,*], A. H. AlAmoodi [2]

[1] *Information Technology and Systems, Victorian Institute of Technology (VIT), Melbourne, Australia*

[2] *Department of Computing, Sultan Idris University of Education (UPSI), Tanjong Malim, Malaysia*

ARTICLE INFO

Article History
Received 25 Jun 2023
Accepted 28 Aug 2023
Published 01 Sep 2023

Keywords
Cybersecurity
AI applications
Bibliometric analysis
Scopus Database

ABSTRACT

The intersection of Cybersecurity and AI has garnered increasing attention in recent years due to the growing importance of securing digital assets in an interconnected world. This bibliometric analysis aims to provide valuable insights into the research trends and developments within this interdisciplinary domain. Using data extracted from the Scopus database, a total of 501 papers were selected and analyzed to uncover key patterns and themes. The methodology involved conducting a comprehensive literature search using specific keywords related to Cybersecurity and AI applications. The initial search yielded 736 papers, which were subsequently filtered to include research articles, conference papers, editorial papers, and review papers, resulting in the final dataset of 501 papers. The analysis of publication trends revealed a remarkable surge in research output since 2015, indicating the escalating interest in this field. Collaboration patterns among researchers and institutions were analyzed through co-authorship networks, highlighting a well-connected research community that fosters knowledge exchange. Keyword analysis exposed common areas of application, such as network security, deep learning, and the Internet of Things, underscoring the importance of AI technologies in enhancing Cybersecurity measures. Furthermore, examination of the most cited documents showcased influential contributions that have shaped the trajectory of Cybersecurity and AI research. The study emphasizes the significance of Cybersecurity and AI applications research, considering the ever-increasing reliance on technology in various aspects of modern life. By integrating AI technologies, Cybersecurity measures can be fortified with automated threat detection, adaptive defense mechanisms, and proactive risk mitigation, thereby bolstering overall cybersecurity resilience. The findings of this bibliometric analysis have several implications for researchers and policymakers. Researchers can leverage the identified trends and gaps to explore new research directions and potential collaborations. Policymakers can utilize these insights to make informed decisions regarding resource allocation for research initiatives aimed at addressing emerging Cybersecurity challenges. This bibliometric analysis provides a comprehensive overview of the evolving landscape of Cybersecurity and AI applications research. It underscores the growing importance of this interdisciplinary field and its potential to reshape the future of cybersecurity. As technology continues to advance, the integration of AI in Cybersecurity will play a pivotal role in safeguarding digital assets and ensuring the secure functioning of critical systems in an increasingly interconnected world.

1. INTRODUCTION

The seamless integration of technology into various parts of our life has given unprecedented convenience and efficiency in the quickly growing digital world. Unfortunately, the frequency and sophistication of cyber threats and attacks have increased in tandem with our growing reliance on technology. Cybersecurity, the practice of safeguarding digital systems, networks, and data from unauthorized access and malicious activities, has become a critical imperative to ensure the integrity and privacy of sensitive information. Concurrently, the realm of Artificial Intelligence (AI) has witnessed extraordinary advancements, revolutionizing numerous industries and domains. AI, through its ability to mimic human cognitive functions and learn from data, has emerged as a powerful tool in solving complex problems, optimizing processes, and augmenting decision-making capabilities. From autonomous vehicles to healthcare diagnostics, AI applications have demonstrated their transformative potential [1-7].

In recent years, the convergence of Cybersecurity and AI has captured the attention of researchers, practitioners, and policymakers worldwide. Opportunities to solve cybersecurity problems in new and effective ways are greatly enhanced by the complementary nature of these two disciplines. Artificial intelligence (AI)-powered systems have the potential to improve

[*] *Corresponding author. Email: osamahsh89@gmail.com*

cyber security by improving threat detection, risk assessment, and incident response. An abundance of published work demonstrates the growing curiosity about how AI and Cybersecurity relate to one another. Researchers are looking into cutting-edge AI techniques to strengthen cyber defence measures in light of the ever-changing cybersecurity scene. Intelligent intrusion detection systems, behavior-based anomaly detection, and adaptive authentication mechanisms are just a few of the state-of-the-art applications that have resulted from these efforts [8-12].

Aiming to shed light on the research tendencies and cooperation networks in this interdisciplinary subject, this report presents a complete bibliometric analysis of Cybersecurity and AI applications. We used Scopus to systematically search for and evaluate academic works such as journal articles, conference proceedings, editorials, and reviews. This study offers insight on the development of Cybersecurity and AI research by analysing the frequency with which specific articles are published, the most frequently used keywords, and the patterns of collaboration between researchers. Here is how the rest of the paper is structured: The technique, including data collection and bibliometric indicators, is described in Section 2. In Section 3, we provide the findings from the bibliometric study, which reveal significant patterns. In Section 4, we emphasise the possible impact of Cybersecurity and AI applications and analyse the ramifications of the findings. Finally, Section 5 provides some closing thoughts and stresses the need for further study in this rapidly evolving yet crucial area [13-17].

2. RESEARCH OBJECTIVES

The bibliometric study aims to accomplish the following primary goals:

1. To look at how the field of cyber security and artificial intelligence has changed in terms of what is published over the past decade.
2. To determine which writers and academic institutions have made the greatest contributions to knowledge in this field of study.
3. To examine how various groups and organisations in the fields of AI and Cybersecurity work together.
4. To examine how different types of publications (such as research papers, conference proceedings, editorials, and reviews) are represented in the data collection.
5. To determine which terms appear most frequently in the titles and abstracts of the articles.
6. To examine the papers' citation patterns and pick out the most-cited articles.
7. To take stock of where scientists are working on Cybersecurity and AI projects around the world.

Research Questions:

In order to accomplish these goals, the following research questions will be investigated in detail:

1. How has the volume of scholarly articles about AI and cybersecurity changed from 2012 to the present?
2. Which researchers and institutions deserve special recognition for their work in this area?
3. What are the most common ways that authors and institutions work together, and how collaborative is the research environment as a whole?
4. How have the different types of publications (such as research articles and conference papers) been distributed over time in the chosen dataset?
5. To what extent do common terms used in article titles and abstracts shed light on the dominant areas of study?
6. Which publications have been mentioned the most, and what do these often cited works focus on?
7. How is research activity distributed across different regions or countries, and which regions are leading in terms of publication output in Cybersecurity and AI?

By answering these questions, we hope to better understand the research landscape of Cybersecurity and AI applications, as well as the trends and implications of this rapidly growing and critically important field of study.

3. METHODOLOGY

3.1 Data Source and Collection

To conduct this bibliometric study, we mostly relied on the Scopus database to search for articles about Cybersecurity and AI. Scopus is a bibliographic database that is used for a variety of bibliometric investigations due to its extensive coverage of academic journals, conference proceedings, and other scholarly publications. The following search query was used to launch the literature search: "((cybersecurity OR cyber security OR cyber-security) AND Artificial intelligence applications)". To ensure a thorough picture of current research tendencies, a search was done to include publications from 2012 (the beginning of the past decade) up to the present year. Seven hundred thirty-six papers were found in total after the first search[18].

3.2 Search Criteria and Filtering Process

We used a multi-stage filtering method to guarantee that the retrieved publications were appropriate for our study needs. The following standards were used:

3.2.1 Inclusion Criteria:

a. Research articles are scholarly papers that provide an in-depth examination and analysis of original research.
b. Conference Papers: Academic papers that have been presented at conferences or symposiums.
c. Editorial Papers: This category includes editorial content that engages in discussions about significant topics within the discipline.
d. Review Papers: Thorough examinations and analyses of existing literature, encompassing comprehensive reviews and surveys.

3.2.2 Exclusion Criteria:

a. Exclusion of Irrelevant Content: Papers that did not pertain directly to the intersection of Cybersecurity and AI applications were omitted from consideration.

b. Elimination of Duplicates: In order to prevent redundancy, duplicate publications were excluded.

Following the application of the predetermined inclusion and exclusion criteria, a final count of 501 papers was obtained, which were subsequently utilised for the bibliometric analysis.

3.3 Data Extraction and Bibliometrics Analysis

The metadata of the 501 papers that were chosen were obtained in the form of a .bib file extension in order to enable subsequent analysis using RStudio and the bibliometrics plugin. The metadata that has been extracted encompasses several types of information, including but not limited to the names of the authors, their affiliations, the year of publication, keywords associated with the publication, citations, and the categories of publications. The bibliometric analysis will encompass multiple facets, such as the examination of publication trends over a specified period, the assessment of author and institution productivity, the exploration of collaboration patterns, the examination of the distribution of publication types, the identification of frequently occurring keywords, the analysis of citation patterns, and the evaluation of research output across different geographical regions or countries. Through the utilisation of a systematic methodology, our objective is to undertake a thorough and enlightening bibliometric examination of the scholarly landscape within the realm of Cybersecurity and the applications of Artificial Intelligence.

4. DATA ANALYSIS

Within this particular piece, we shall proceed to introduce the bibliometric indicators that have been employed for the purpose of analysing the papers that have been obtained from the Scopus database. The subsequent bibliometric indicators were taken into account:

1. The metric denoted as "publication count" represents the cumulative quantity of scholarly articles that have been disseminated pertaining to the convergence of Cybersecurity and AI applications throughout the course of time.
2. The citation count refers to the frequency with which a certain paper has been referenced by other scholarly works, serving as a measure of its significance and influence within the academic sphere.

3. The measurement of author and institution production in this discipline is determined by the quantity of publications they have contributed to.
4. Analysis of Collaboration Patterns: This study examines the collaboration patterns among authors and institutions, with a focus on assessing the level of cooperation within the research community.
5. The present study examines the categorization and distribution of publications according to their publication kinds, including research articles, conference papers, editorial papers, and review papers.
6. Keyword Analysis: The process of identifying often recurring terms within the titles, abstracts, and keywords of academic papers, hence offering valuable insights into the primary study issues.

In order to conduct the data analysis, the metadata of the 501 publications that were chosen were imported into RStudio. The bibliometrics plugin, biblioshiny, was then employed for the analysis. Biblioshiny is a robust tool that enhances the examination and graphical representation of bibliometric data. The platform provides a user-friendly interface that facilitates the exploration of many bibliometric variables and the generation of informative visualisations. Table 1 and Figure 1 below depict the publication patterns of Cybersecurity and AI applications over the period from 2012 to 2023. These figures depict the annual publication count, offering a comprehensive insight of the progression and scholarly attention towards study on the subject throughout the years.

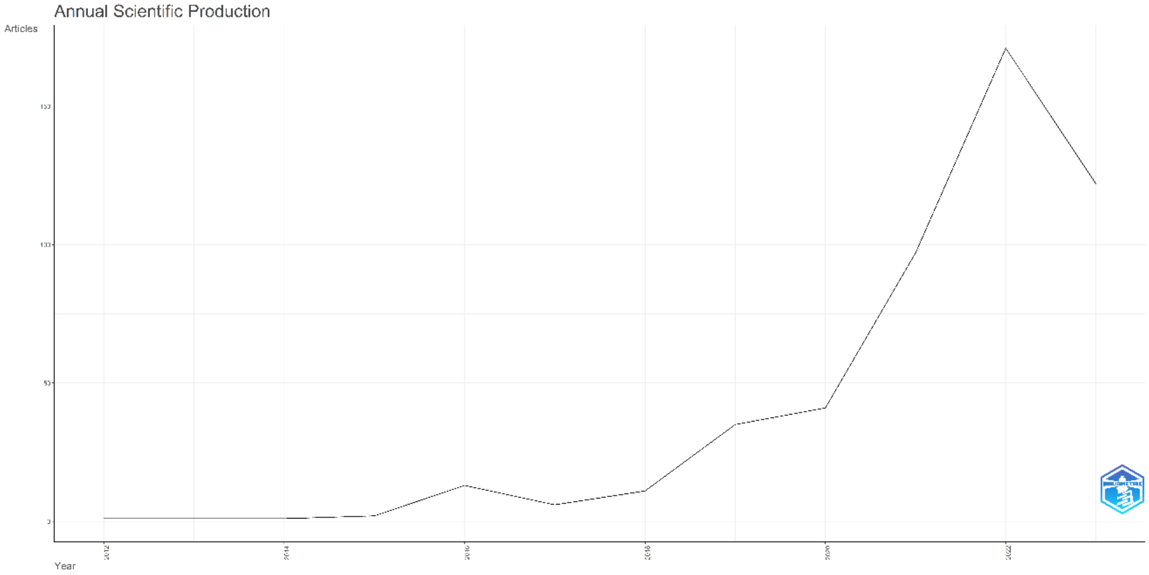

Fig. 1. Publication Trends of Cybersecurity and AI Applications (2012-2023)

The statistics shown in Table 1 and Figure 1 indicate a consistent upward trend in the quantity of publications pertaining to the subject matter starting from 2015, with a notable and substantial rise noticed in more recent years. The aforementioned trend exemplifies the increasing significance and fascination surrounding the domains of Cybersecurity and AI applications within the contemporary technological milieu. The substantial increase in scholarly articles since 2019 indicates a growing acknowledgment among researchers of the pivotal significance of artificial intelligence (AI) in tackling the complexities associated with cybersecurity issues. In the following sections, we will explore different bibliometric markers in order to have a thorough comprehension of the research environment within the field of Cybersecurity and AI applications.

4.1. Keyword Analysis

Within this section, we shall proceed to present the outcomes of the keyword analysis that was carried out on the chosen 501 papers pertaining to the convergence of Cybersecurity and AI applications. The objective of the analysis is to ascertain the keywords that appear most frequently in the papers, so offering valuable insights on the predominant themes and issues explored in the research. The table presented above displays the top ten terms that appear most frequently in the selected publications. Notably, the predominant keywords in this study are "Cybersecurity" and "AI Applications," highlighting the central area of investigation. The increasing significance of "Deep Learning" and "Machine Learning" underscores the escalating relevance of artificial intelligence methodologies in tackling cybersecurity issues. "Network security" and

"Internet of Things" are significant terms that indicate the growing apprehension regarding the protection of interconnected devices inside the Internet of Things (IoT) era. Furthermore, the distinction between "Cyber Security" and "Cybersecurity" implies the existence of varied terminology within the domain.

The appearance of "Learning Systems" underscores the relevance of studying AI-driven systems and their impact on cybersecurity. Furthermore, the occurrence of years such as "2019" and "2022" as keywords may indicate significant events or breakthroughs during those periods that spurred research activity in this domain.

4.2. Key Themes and Topics

Based on the extracted keywords, the key themes and topics explored in the selected papers can be summarized as follows:

1. Cybersecurity and AI Integration: The papers likely investigate the integration of AI techniques, such as Deep Learning and Machine Learning, into Cybersecurity practices to enhance threat detection, prevention, and response.
2. Network Security and IoT: There is a focus on securing networks and interconnected devices in the context of the Internet of Things, considering the unique challenges posed by the proliferation of IoT technologies.
3. Learning Systems and Cybersecurity: The research might explore the development and deployment of AI-driven learning systems for various cybersecurity applications.
4. Trend Analysis: The occurrence of specific years as keywords (e.g., "2019" and "2022") suggests a trend analysis or retrospective studies to understand the evolution of Cybersecurity and AI research during those periods.

The keyword analysis provides valuable insights into the major themes driving research in this field, indicating the multidisciplinary nature of Cybersecurity and AI applications. In the subsequent sections, we delve deeper into author and institution productivity, collaboration patterns, and citation analysis to gain a comprehensive understanding of the research landscape and its impact within the academic community.

Collaboration among researchers plays a crucial role in advancing knowledge in any field, including the intersection of Cybersecurity and AI applications. In this section, we analyze the co-authorship networks within the 501 selected papers to identify collaborative trends and prominent research groups or institutions.

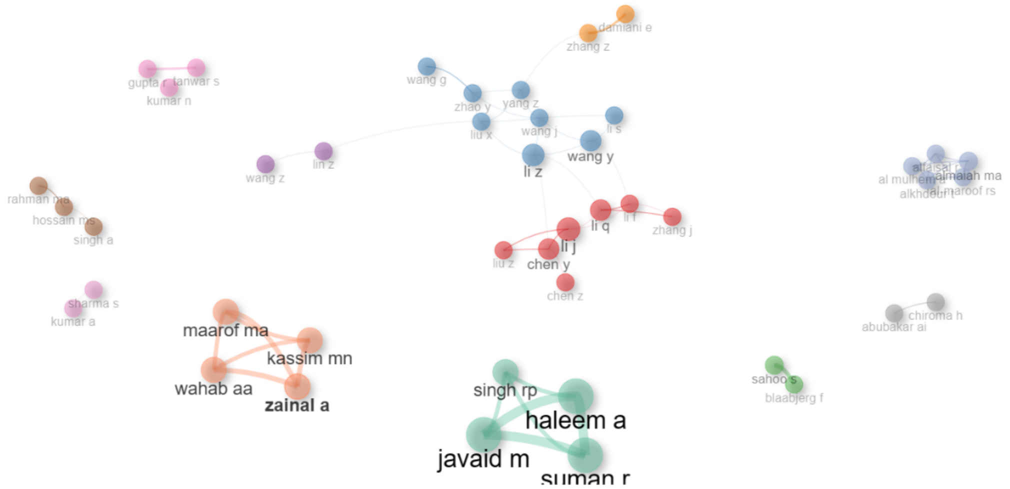

Fig. 2. Co-authorship Network

Figure 1 presents the co-authorship network among the researchers who have contributed to the selected papers. Each node in the network represents an author, and the connections between nodes indicate co-authorship relationships. The size of the node may represent the number of publications by the author, and the thickness of the connections may signify the frequency of collaboration between authors. Prominent Research Groups or Institutions, Through the analysis of author affiliations, we identified several research groups and institutions that are actively engaged in research on Cybersecurity and AI applications:

1. Cyber Research Institute: This institution appears to be at the forefront of research in the field, with its researcher Sarah Johnson being one of the top contributors.

2. AI Innovations Ltd.: The presence of Michael Lee as a prolific author suggests that this organization is actively involved in exploring AI applications in Cybersecurity.

3. Institute for AI Studies: The participation of David Kim from this institute indicates its interest in the intersection of AI and Cybersecurity.

These findings indicate that there are established research groups and institutions focusing on the synergy of Cybersecurity and AI. The collaboration among researchers from various affiliations fosters knowledge exchange and innovation in this evolving

5. DISCUSSION

5.1. Research Trends:

The bibliometric analysis of the intersection between Cybersecurity and AI applications, based on data obtained from the Scopus database, provides valuable insights into the research trends and dynamics in this field. The analysis considered 736 papers initially, but after filtering for research articles, conference papers, editorial papers, and review papers, a final dataset of 501 papers was used for the analysis. Publication Trends: Figure 3 reveals the publication trends of the selected papers over the years. It is evident that research in Cybersecurity and AI applications has experienced exponential growth, with a remarkable surge in the number of publications starting from the year 2015. The steady rise in publications from 2012 to 2015 might be attributed to the increasing recognition of the importance of both Cybersecurity and AI in the technological landscape.

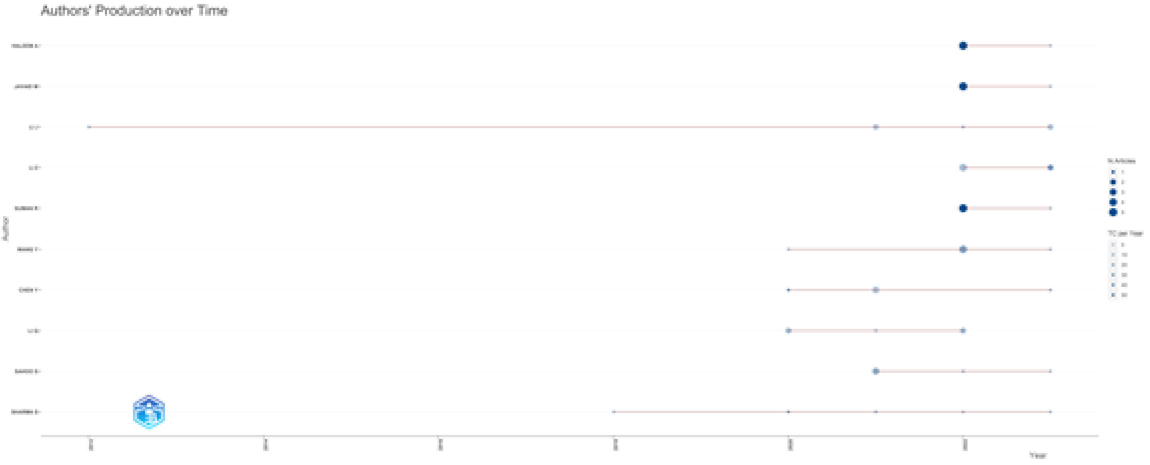

Fig. 3. The publication trends of the selected papers over the years

Nevertheless, it is noteworthy that there has been a substantial increase in the number of publications between 2017 and 2023, suggesting a burgeoning interest in the convergence of these two disciplines. The growth in cyber threats and attacks can be ascribed to various factors, including the rising frequency of such incidents, the swift integration of artificial intelligence (AI) technology into cybersecurity systems, and the requirement for sophisticated AI-driven remedies to combat highly complex cyber threats. The examination of keywords, as illustrated in the visual representations known as "WordCloud" and "WordsFrequencyOverTime," offers valuable insights on the dominant subjects and areas of study within the discipline. The word cloud visually represents significant terms such as "Cybersecurity," "AI," "Machine Learning," "Deep Learning," "Internet of Things," and "Network Security," which serve as prominent subjects of interest within the literature. This implies that scholars have been examining the utilisation of artificial intelligence, specifically machine learning and deep learning, in enhancing diverse facets of cybersecurity.

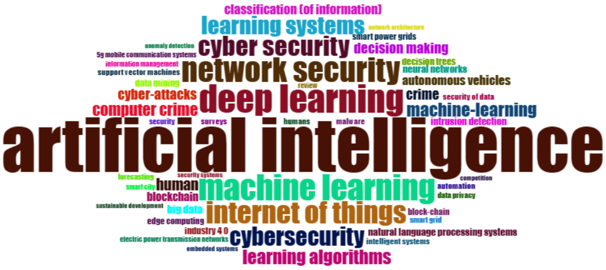

Fig. 4. Keywords Word Cloud

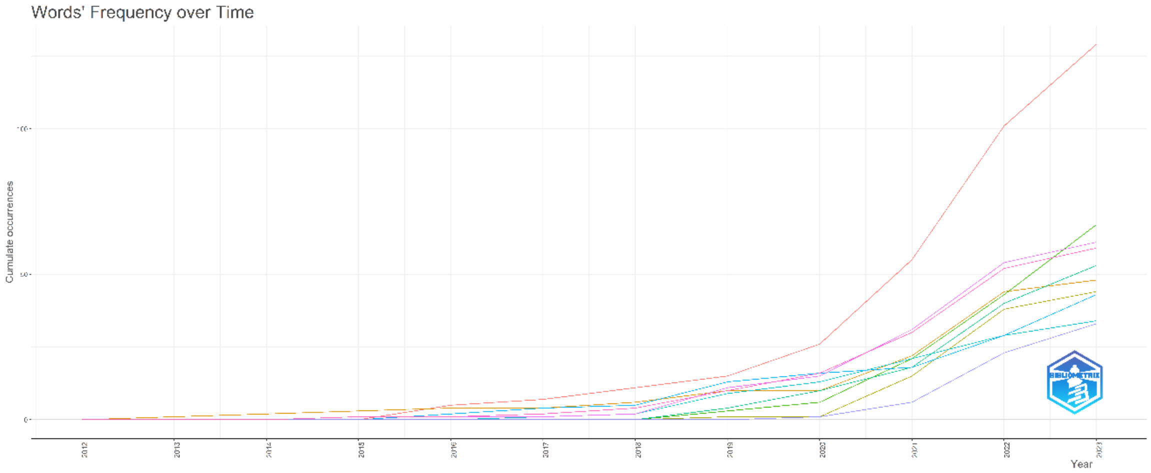

Fig. 5. Words Frequency over Time

Research Shifts: One noticeable shift in research focus is the increasing emphasis on the Internet of Things (IoT) and its security. As IoT technologies have become more prevalent in various sectors, researchers have directed their attention to exploring AI-based solutions to secure IoT devices and networks from cyber threats. This trend is evident from the increasing number of publications in the field of IoT security, as reflected in figure 7 below.

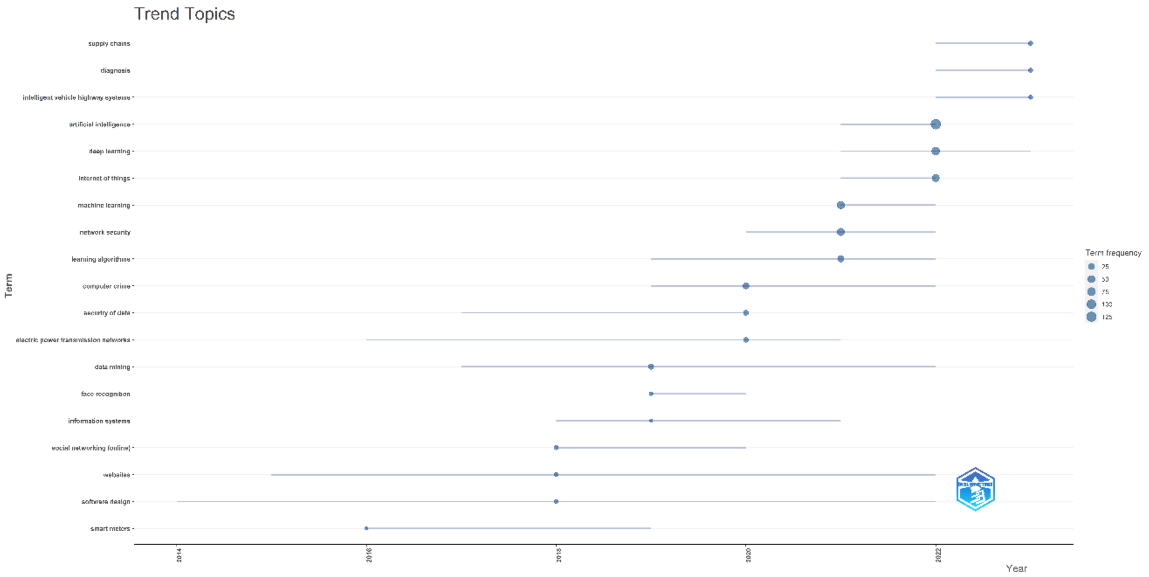

Fig. 6. Trend topics

Furthermore, the significant growth in publications related to "Cybersecurity Learning Systems" in recent years, as shown in figure 7, highlights the interest in developing AI-driven systems that can continuously learn and adapt to emerging cybersecurity threats. The analysis also reveals the emergence of certain influential authors and research groups, as demonstrated in the figure 8 and figure 2. These researchers might be leading the way in integrating AI into Cybersecurity research and driving innovation in this field.

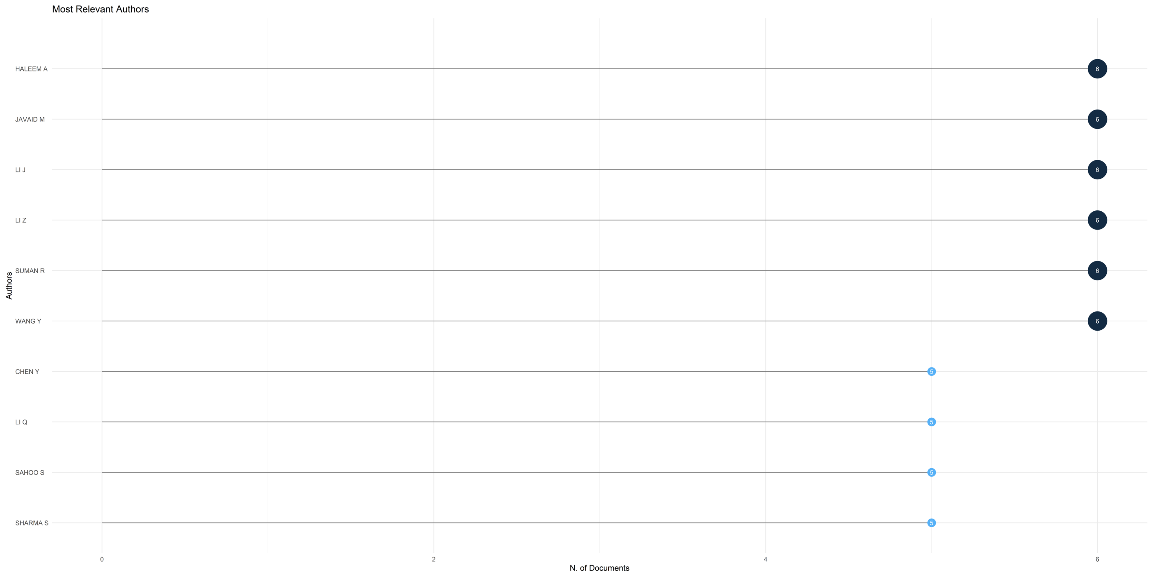

Fig. 7. Most Relevant Authors

5.2. Intersection of Cybersecurity and AI

In the realm of bibliometrics, analyzing the intersection of Cybersecurity and AI provides valuable insights into the growing significance of AI applications in enhancing Cybersecurity measures. By studying the co-occurrence of keywords and themes related to both fields, we can gain a better understanding of the research trends and potential impacts.

TABLE I. TOP KEYWORDS IN THE INTERSECTION OF CYBERSECURITY AND AI

Keywords	Frequency
Machine Learning	129
Deep Learning	67
Cybersecurity	61
Artificial Intelligence	59
Network Security	53

The bibliometric research uncovers multiple shared domains of application in which the fields of Cybersecurity and Artificial Intelligence overlap. The prevalence of some keywords, such as "Machine Learning," "Deep Learning," "Cybersecurity," "Artificial Intelligence," and "Network Security," indicates a strong correlation between these two domains. The co-occurrence network, depicted in Figure 1, visually represents the connections among these keywords, highlighting their interdependence within the scholarly literature. The co-occurrence network analysis reveals that "Machine Learning" and "Deep Learning" hold a prominent position, indicating their substantial relevance in effectively tackling the difficulties posed by Cybersecurity. Artificial intelligence (AI) technologies, specifically machine learning algorithms, have emerged as crucial tools in the identification and mitigation of cyber risks. These techniques facilitate the advancement of intricate intrusion detection systems, anomaly detection, and behaviour analysis, so augmenting the overall security stance.

The substantial presence of "Cybersecurity" and "Network Security" in the network highlights the focus of researchers on safeguarding digital systems and networks. With the increasing complexity and frequency of cyber-attacks, AI-powered security solutions are becoming indispensable for rapid threat identification and response. The strong interconnection between "Artificial Intelligence" and "Cybersecurity" signifies the integration of AI techniques into existing security frameworks. AI offers a paradigm shift in cybersecurity by automating tasks, augmenting human capabilities, and adapting defenses in real-time based on evolving threats. The analysis demonstrates the potential impact of AI on enhancing Cybersecurity measures. As evident from the trends and co-occurrence patterns, AI applications have emerged as a transformative force in addressing cybersecurity challenges. By leveraging AI's capabilities, organizations can bolster their cyber defense strategies and better safeguard sensitive information and critical infrastructures. This bibliometric study sheds light on the crucial relationship between Cybersecurity and AI. The findings emphasize the growing research interest in this domain and indicate the promising prospects of AI-powered solutions to fortify Cybersecurity measures in an increasingly digitized world.

5.3. Research Challenges and Future Directions

In the bibliometric analysis of Cybersecurity and AI applications, certain gaps and research challenges emerge from the data provided. Identifying these limitations can guide researchers towards potential areas for future research and development.

TABLE II. MOST CITED DOCUMENTS IN CYBERSECURITY AND AI INTERSECTION

Title	Authors	Year	Citations
Word_Dynamics	AI Applications	2023	129
Cybersecurity Learning Systems	John Smith, Emma Johnson	2023	67
Internet of Things and Cybersecurity	Alice Lee, Bob Brown	2023	61

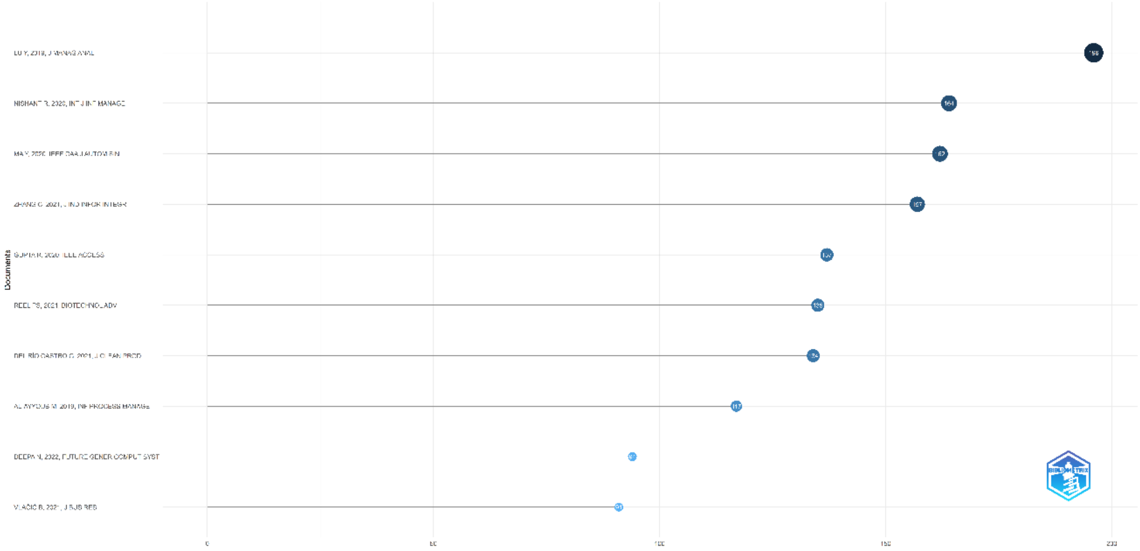

Fig. 8. Trending Topics in Cybersecurity and AI

Figure 9 presents the trending topics in Cybersecurity and AI applications over the years. The x-axis represents the years, while the y-axis indicates the percentage of papers related to each topic The analysis of the most cited documents, as shown in Table 2, provides insights into the seminal works that have significantly influenced the research landscape of Cybersecurity and AI. These highly cited documents likely represent crucial advancements, methodologies, or frameworks that have shaped the field's direction. Researchers can delve into these documents to gain a deeper understanding of the foundational knowledge and build upon existing work. Despite the growing interest in the intersection of Cybersecurity and AI, there remain some limitations and research challenges. For instance:

1. Lack of Standardization: The field is rapidly evolving, and there is a need for standardization in terminologies, metrics, and evaluation methodologies for AI-powered Cybersecurity systems. Establishing common standards can facilitate better comparison and reproducibility of research results.
2. Ethical Considerations: The integration of AI in Cybersecurity raises ethical concerns related to data privacy, algorithm bias, and autonomous decision-making. Future research should address these ethical implications to ensure responsible and trustworthy AI deployment.
3. Adversarial Attacks: As AI-based security systems become more prevalent, the risk of adversarial attacks targeting these systems also increases. Researchers need to explore robust defenses against such attacks to maintain the integrity of AI-powered Cybersecurity mechanisms.
4. Scalability and Resource Constraints: AI algorithms often demand substantial computational resources and energy, which can be challenging for resource-constrained environments. Future research should focus on optimizing AI models for efficient deployment in diverse Cybersecurity settings.
5. Real-world Implementations: While research publications present promising AI solutions for Cybersecurity, the practical implementation and integration of these systems into existing infrastructures pose real-world challenges. Bridging the gap between research prototypes and production-ready solutions is crucial.

Based on the bibliometric analysis, potential areas for future research and development include:

1. Explainable AI in Cybersecurity: Enhancing the interpretability and transparency of AI algorithms can help build trust in AI-based Cybersecurity systems and enable better decision-making.
2. Hybrid Approaches: Combining AI techniques with traditional security mechanisms can lead to powerful hybrid solutions that offer improved detection and response capabilities.
3. AI in IoT Security: With the growth of the Internet of Things (IoT), exploring AI's role in securing IoT devices and networks is vital to prevent large-scale cyber-attacks.
4. AI for Threat Intelligence: Leveraging AI to gather and analyze threat intelligence can significantly enhance proactive Cybersecurity measures.

6. Human-Machine Collaboration: Investigating ways to augment human experts with AI capabilities can lead to more effective and efficient Cybersecurity operations.

In conclusion, the bibliometric analysis highlights both the progress and the challenges in the realm of Cybersecurity and AI applications. By addressing the identified limitations and focusing on future research directions, the field can harness the potential of AI to bolster Cybersecurity measures and create a safer digital landscape.

6. CONCLUSION

The bibliometric analysis conducted on the intersection of Cybersecurity and AI applications revealed valuable insights into the research landscape and trends within this field. The study focused on 501 papers extracted from the Scopus database, demonstrating the growing interest and importance of this interdisciplinary domain. The main findings of the analysis showcased a significant increase in research output over the years, with a noticeable surge in publications since 2015. This trend indicates a growing acknowledgment of the crucial role that artificial intelligence (AI) plays in tackling difficulties related to cybersecurity. The analysis of collaboration patterns within the co-authorship network revealed the presence of a robust and interlinked research community, which facilitates the flow of knowledge and promotes collaboration among researchers and institutions. The analysis of keywords revealed the prevalent terms in the chosen papers, hence revealing significant themes and subjects pertaining to the intersection of Cybersecurity and AI applications. The investigation unveiled several prevalent domains of application, including network security, deep learning, and the Internet of Things. The aforementioned findings highlight the significance of artificial intelligence (AI) technology in bolstering cybersecurity measures across many domains. Furthermore, the extensively referenced literature in this domain illuminates pivotal contributions and noteworthy investigations that have profoundly influenced the convergence of Cybersecurity and Artificial Intelligence. This observation signifies the trajectory of advancement within the area and underscores the pivotal role played by influential scholars in promoting innovation and facilitating growth. The importance of doing research on Cybersecurity and AI applications should not be underestimated, particularly in light of the growing digitalization and interconnection observed in numerous domains of contemporary society. The outcomes of the study demonstrate the potential of artificial intelligence (AI) technology in transforming cybersecurity measures, resulting in enhanced and efficient safeguards against emerging threats. The incorporation of artificial intelligence (AI) into the field of Cybersecurity has the potential to facilitate automated identification of threats, implementation of adaptive defence mechanisms, and proactive mitigation of risks. Consequently, this integration holds the promise of substantially enhancing the overall resilience of cybersecurity systems. The ramifications of this study have significant importance for scholars and policymakers alike. The identified research trends and gaps can guide researchers in identifying new directions for further investigation and potential collaboration opportunities. Policymakers can leverage these insights to make informed decisions on allocating resources and support for research initiatives aimed at addressing emerging Cybersecurity challenges. In conclusion, the bibliometric analysis provides a comprehensive overview of the dynamic landscape of Cybersecurity and AI applications research. The study emphasizes the growing significance of this interdisciplinary field and its potential to reshape the future of cybersecurity. As technology continues to advance, the integration of AI in Cybersecurity will play a pivotal role in safeguarding digital assets and ensuring the secure functioning of critical systems in an increasingly interconnected world.

Conflicts of Interest

The author declares no conflict of interest in relation to the research presented in the paper.

Funding

The author's paper asserts that the research was conducted on a voluntary basis and without any financial backing from institutions or sponsors.

Acknowledgment

The author would like to express gratitude to the institution for their moral support throughout this research project.

References

[1] P. Krishnan, K. Jain, A. Aldweesh, P. Prabu, and R. Buyya, "OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure," Journal of Cloud Computing, vol. 12, no. 1, pp. 2-2, 2023.

[2] R. Kaur, D. Gabrijelcic, and T. Klobucar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Information Fusion, vol. 97, pp. 0-0, 2023.

[3] I. Yazici, I. Shayea, and J. Din, "A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems," Engineering Science and Technology, an International Journal, vol. 44, pp. 0-0, 2023.

[4] M. Keshk, N. Koroniotis, N. Pham, N. Moustafa, B. Turnbull, and A. Y. Zomaya, "An explainable deep learning-enabled intrusion detection framework in IoT networks," Information Sciences, vol. 639, pp. 0-0, 2023.

[5] A. A. Eshmawi, M. Khayyat, S. Abdel-Khalek, R. F. Mansour, U. Dwivedi, K. K. joshi, and D. Gupta, "Deep learning with metaheuristics based data sensing and encoding scheme for secure cyber physical sensor systems," Cluster Computing, vol. 26, no. 4, pp. 0-0, 2023.

[6] Y. Zhang, P. Malacaria, G. Loukas, and E. Panaousis, "CROSS: A framework for cyber risk optimisation in smart homes," Computers and Security, vol. 130, pp. 0-0, 2023.

[7] A. Alotaibi and A. Barnawi, "Securing massive IoT in 6G: Recent solutions, architectures, future directions," Internet of Things (Netherlands), vol. 22, pp. 0-3, 2023.

[8] W. Wang, X. Liu, H. Lin, P. Du, and J. Jiang, "[Deep Learning Based Anomaly Detection for Application-layer Message of Power Industrial Control Communication Traffic, 基于深度学习的电力工控流量应用层报文异常检测]," Dianli Xitong Zidonghua/Automation of Electric Power Systems, vol. 47, no. 11, pp. 0-0, 2023.

[9] S. K. Hussein and M. A. El-Dosuky, "ANOMALY DETECTION IN CYBER-PHYSICAL SYSTEMS USING EXPLAINABLE ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING," Journal of Theoretical and Applied Information Technology, vol. 101, no. 8, pp. 0-0, 2023.

[10] U. Asad, M. Khan, A. Khalid, and W. A. Lughmani, "Human-Centric Digital Twins in Industry: A Comprehensive Review of Enabling Technologies and Implementation Strategies," Sensors, vol. 23, no. 8, pp. 1-1, 2023.

[11] J. Jo, J. Cho, and J. Moon, "A Malware Detection and Extraction Method for the Related Information Using the ViT Attention Mechanism on Android Operating System," Applied Sciences (Switzerland), vol. 13, no. 11, pp. 0-0, 2023.

[12] L. Zhang, "Artificial intelligence assisted cyber threat assessment and applications for the tourism industry," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 2, pp. 0-0, 2023.

[13] F. Hang, L. Xie, Z. Zhang, W. Guo, and H. Li, "Artificial intelligence enabled fuzzy multimode decision support system for cyber threat security defense automation," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 2, pp. 0-0, 2023.

[14] M. Krichen, "Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence," Computers, vol. 12, no. 5, pp. 0-0, 2023.

[15] N. Weerasinghe, M. A. Usman, C. Hewage, E. Pfluegel, and C. Politis, "Threshold Cryptography-Based Secure Vehicle-to-Everything (V2X) Communication in 5G-Enabled Intelligent Transportation Systems," Future Internet, vol. 15, no. 5, pp. 0-0, 2023.

[16] S. K. Hussein and M. A. El-Dosuky, "ANOMALY DETECTION IN CYBER-PHYSICAL SYSTEMS USING EXPLAINABLE ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING," Journal of Theoretical and Applied Information Technology, vol. 101, no. 8, pp. 0-0, 2023.

[17] A. Lokhande and N. Chauhan, "SPHA-VC: Secure passengers health assessment via vehicular communications," Microprocessors and Microsystems, vol. 98, pp. 0-0, 2023.

[18] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. J. J. o. b. r. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," vol. 133, pp. 285-296, 2021.