Journal of Process Management and New Technologies
Vol. 14, Issue 1-2, 2026, pp. 133-152

BIBLIOMETRIC RESEARCH IN THE FIELD OF CYBERSECURITY: FOCUS ON ARTIFICIAL INTELLIGENCE AND ATTACK DETECTION

Aleksandar ŠIJAN[1*], Luka ILIĆ[2], Dejan VIDUKA[3], Chulung LEE[4], Bratislav PREDIĆ[5]

[1]*Faculty of Electronic Engineering, University of Niš, Niš, Serbia, aleksandar@mef.edu.rs*
https://orcid.org/0000-0002-7133-5700

[2]*Faculty of Electronic Engineering, University of Niš, Niš, Serbia, luka.ilic@mef.edu.rs*
https://orcid.org/0009-0004-5577-4713

[3]*Faculty of Information Technologies, Alfa BK University, Belgrade, Serbia, dejan.viduka@alfa.edu.rs*
https://orcid.org/0000-0001-9147-8103

[4]*Department of Industrial and Management Engineering, Korea University, Seoul, Republic of Korea, leecu@korea.ac.kr*
https://orcid.org/0000-0002-2041-0221

[5]*Faculty of Electronic Engineering, University of Niš, Niš, Serbia, bpredic@gmail.com*
https://orcid.org/0000-0002-3679-5058

Abstract: *This paper presents a comprehensive bibliometric analysis of the field of cybersecurity, with a specific focus on the application of artificial intelligence (AI) in attack detection. The study aims to provide insights into the trends, research areas, and key contributions in this rapidly evolving field, while also exploring the theoretical underpinnings of security and the challenges associated with the implementation of AI in attack detection. Theoretical frameworks in cybersecurity emphasize the importance of robust and adaptive defence mechanisms, which AI technologies strive to enhance. Despite these advancements, the dynamic nature of cyber threats necessitates continuous innovation and interdisciplinary collaboration. The findings of this bibliometric analysis provide valuable insights into the development and current state of research at the intersection of cybersecurity and AI. The study highlights the most influential works, prominent authors, and emerging trends in this critical area of study. This comprehensive analysis aims to serve as a valuable resource for researchers, practitioners, and policymakers, fostering a deeper understanding of how AI technologies can be effectively leveraged to enhance cybersecurity measures and address the complexities of modern cyber threats.*

Keywords: *Artificial intelligence (AI), attack detection, cybersecurity, web of science, bibliometric analysis.*

Review paper
Received: 29.03.2026
Accepted: 28.05.2026
Available online: 21.06.2026
DOI: 10.5937/jpmnt14-66097

* Corresponding author

1. Introduction

Cybersecurity is a key area of research in the digital age (Allahrakha, 2023), where the protection of information systems from various threats and attacks is becoming increasingly important (Spremić & Šimunić, 2018). With the development of technology and the increasing number of connected devices, threats in cyberspace are becoming more complex and sophisticated (Pandey et al., 2022). Traditional approaches to the protection of information systems are often not effective enough to respond to these challenges (Bélanger & Crossler, 2011), which is why there is a need for more innovative solutions.

Artificial intelligence (AI) stands out as a revolutionary technology (Makridakis, 2017) that can significantly improve the detection and prevention of cyber-attacks (Kumar et al., 2023). The application of AI in cybersecurity enables faster identification of threats, automatic analysis of large amounts of data and proactive response to attacks (Bécue et al., 2021). Machine learning algorithms, deep learning and other AI techniques are becoming necessary tools to improve the security of information systems (Gupta et al., 2022).

Despite the great potential, the application of artificial intelligence in cybersecurity brings with it certain challenges (Sobb et al., 2020). Continued research and analysis are needed to understand all the possibilities and limitations of these technologies. Also, with the growing number of research and publications in this field, there is a need for a comprehensive analysis of existing works in order to identify key trends, the most influential researchers and directions for future research.

Bibliometric research (McBurney & Novak, 2002) provides valuable insights into the evolution of a scientific discipline, mapping research flows and identifying the most influential works and authors (Pessin et al., 2022). This paper aims to investigate current trends in the field of cybersecurity with a focus on artificial intelligence and attack detection through bibliometric analysis. By analyzing the existing literature, the main thematic units, methodological approaches and key contributions in this field will be identified.

It is expected that the results of this analysis will contribute to a better understanding of the current state and future directions of research in the application of artificial intelligence to improve cybersecurity, which will facilitate the further development and application of these technologies in practice.

1.1. Introduction to cybersecurity

Cybersecurity is a key aspect of protecting information systems (Borky & Bradley, 2019), networks and data from unauthorized access, use, disclosure, disruption, modification or destruction (Alhassan & Adjei-Quaye, 2017; Gunduz & Das, 2020; Perwej et al., 2021; Singh et al., 2014). Considering the rapid progress of technology and the increasing dependence of society on digital systems (Hassani et al., 2021; Popkova et al., 2022), the importance of cybersecurity is becoming the number one topic (Senol & Karacuha, 2020). The main objectives of cybersecurity are to preserve the confidentiality, integrity and availability of data (Gunduz & Das, 2020).

1.2. The role of artificial intelligence in cybersecurity

Artificial intelligence (AI) has become a key component of modern cybersecurity systems (Hassani et al., 2020; Sarker et al., 2021). AI techniques, such as machine learning, deep learning, and natural language processing algorithms, enable more efficient analysis of large amounts of data (Deng & Liu, 2018), detecting anomalies and predicting potential threats (Bécue et al., 2021; Elmrabit et al., 2020; Gudala et al., 2019; Shah, 2021).

- Machine learning (ML) (Dasgupta et al., 2022): ML techniques allow systems to learn from data and make decisions without explicit programming. In cybersecurity, ML is

used to detect malicious activity through the analysis of behavior patterns in network traffic.

- Deep learning (DL) (Ilić et al., 2024): DL models, such as neural networks, provide more advanced capabilities for recognizing complex patterns in data. These models are particularly useful for identifying sophisticated attacks lurking in large datasets.
- Natural Language Processing (NLP) (Salloum et al., 2021): NLP enables the analysis and understanding of textual data, which is useful for detecting phishing attacks, analyzing malicious code, and identifying threats in real time

1.3. Attack detection using artificial intelligence

Attack detection is a key aspect of cybersecurity (Dissanayake, 2021). Traditional detection methods have limited effectiveness in dealing with new and unknown threats (Patcha & Park, 2007). AI techniques offer more advanced approaches to attack detection:

- Anomaly detection (Elmrabit et al., 2020): Using ML algorithms, anomaly detection identifies unusual patterns in network traffic that may indicate potential attacks.
- Predictive analytics (Yeboah-Ofori et al., 2021): AI models can predict potential threats by analyzing historical data and identifying trends that precede attacks.
- Automated threat response (Sarker, 2024): By integrating AI with automated systems, it is possible to respond quickly to identified threats, thereby minimizing potential damage.

1.4. Challenges and threats in cybersecurity

Although AI offers many advantages in cybersecurity, there are also significant challenges and threats (Nadella & Gonaygunta, 2024):

- False positives and negatives: AI systems can generate false positives (Bieniasz & Szczypiorski, 2021) (detection of non-existent threats) and false negatives (missing real threats), which can compromise detection efficiency.
- Attacks on AI systems (Qiu et al., 2019): Attackers can try to fool AI models using techniques such as adversarial attacks, where input data is manipulated to trick the model.
- Privacy and Ethics (Mylrea & Robinson, 2023): Using large datasets to train AI models may pose a risk to user privacy (Yazdinejad et al., 2024). Also, ethical issues related to automatic decision making and responsibility for errors must be carefully considered.
- Maintenance and updating (Brundage et al., 2018): AI models require continuous updating and training with new data to remain effective against new threats.

2. Methodology

To systematically examine the intersection between artificial intelligence (AI) and cyber security, this research employs a methodological approach rooted in scientometrics and bibliometric analysis. These methodologies are essential for the systematic evaluation of scientific work and the identification of emerging research trends. Scientometrics involves the quantitative analysis of scientific publications, utilizing various metrics to assess the impact and productivity of researchers, institutions, and countries. Bibliometric analysis, a specialized branch of scientometrics, focuses on the examination of bibliographic data and citation patterns to explore the structure and dynamics of scientific disciplines. An important aspect of this approach is the reliance on well-defined search strategies and carefully selected keywords. The effectiveness of bibliometric analysis largely depends on the accuracy and comprehensiveness

of the keywords used to query academic databases. This means that the scope of the research is inherently influenced by the chosen keywords, and as a result, it is always possible that certain high-quality papers or prominent researchers may not be fully represented. To mitigate this limitation, the methodological framework of this study includes a detailed definition of the search strategy and the specific keywords employed, ensuring a robust and comprehensive analysis.

While bibliometric analysis provides substantial insights into the structural aspects of a scientific domain and can highlight areas of high research potential, it is important to acknowledge that it focuses primarily on the interpretation of available data. Therefore, the quality of the results depends on the initial search parameters and the coverage of the databases used. One notable limitation is the potential bias introduced by reliance on specific databases, such as Web of Science, which may exclude relevant works indexed in other sources like Scopus or Google Scholar. Despite these limitations, scientometrics and bibliometric analysis remain invaluable tools in scientific research, offering a quantitative foundation for assessing research performance and guiding future investigations. This is particularly crucial for researchers, policymakers, and institutions aiming to advance scientific knowledge and innovation.

The following sections outline the framework, research question, and sources utilized in this review. Through the careful selection and analysis of pertinent scientific literature, this study seeks to provide meaningful insights into current trends and research progress within this critical area.

2.1. Methodological framework of the research

In this part, the methodology of the review of works on the subject of artificial intelligence in cybersecurity and attack detection is presented (Salih et al., 2021). This research study used the Web of Science database (Clarivate Analytics Web of Science Core Collection: Science Citation Index Expanded (SCI-EXPANDED)) (Liu, 2019). Science Citation Index Expanded (SCI-Expanded) is a citation index originally developed by the Institute for Scientific Information and created by Eugene Garfield. The Science Citation Index was officially launched in 1964 (Masic, 2016), and today it is one of the leading databases that indexes work from scientific disciplines: Science, medicine, and technology, providing an important tool for monitoring the citation of scientific works in those fields. In the set of data exported from this database, there are journals of publishers such as: IEEE(364), ACM(63), MDPI(62), FRONTIERS(15), PEERJ(3), which are represented by a total of 507 papers, while the rest of the papers are independent publishers. The review was conducted according to the PRISMA framework shown in Figure 1 (Page et al., 2021).

2.2. Defining the research question

In this step, the research question is defined. According to Arksey and O'Malley (2005), the aim of this research is to examine the available scientific papers in order to determine the degree of representation of research on the topic of artificial intelligence and its impact on cybersecurity.

Our research question is: "What has been researched in the last few years on the topic of artificial intelligence in cybersecurity and what are the trends in this field?"

2.3. Defining search sources

The Clarivate Analytics Web of Science (WoS) database was selected for the review of papers on the topic of artificial intelligence in cybersecurity. The initial search showed that WoS contains a significant number of relevant scientific papers (total of 57,143 papers found in our search), which justifies the use of this database as a data source, but it was taken into account

that similar research was already done in the Scopus database. These two databases are considered the leading databases in this field (Zhu & Liu, 2020b). And the initial point in choosing the topic was the paper (Ahmed et al., 2022) which deals with similar research but conducted in the Scopus database, so it is interesting to see the difference between the two researches using different databases.

2.4. Defining a search

Keywords and their combinations are defined here. Based on the research, keywords such as "cybersecurity", "cyber security", "cyber-security", "attack detection" and "Artificial intelligence" were selected. Three terms for cybersecurity were used, in order to include as many works as possible, regardless of the definition of this term. The search was conducted using the following query: "((cybersecurity OR cyber security OR cyber-security OR attack detection) AND Artificial intelligence)". The search was performed in all fields (All Fields), not only in the title and keywords, which is often the case in the practice of conducting such analyses. This was the first step in the literature review on this topic. In subsequent steps, the results were reduced using filters to obtain only relevant papers (the final number of papers we use in this analysis is 879). Defining the strategy was done by following and at the same time adapting to our needs the work (Albahri & AlAmoodi, 2023) published in 2023 with similar goals by analysing the Scopus database.

2.5. Conducting a search

The search process was carried out according to the defined query from the previous step. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines were used to comprehensively summarize previously published papers (Liberati et al., 2009). The PRISMA guidelines include three phases: identification, review and inclusion (Page et al., 2021). The search of works and data collection was carried out on June 13, 2024. The next step was to assess the quality of the data found according to the Kitchenham, Mendes and Travassos (2007) criteria. After a detailed review of the selected papers, the initial set of publications was further reduced.

2.6. Primary analysis of scientific papers

The necessary data were extracted according to the research question, and the entire search and selection process is shown in Figure 1. The papers were reviewed according to: Most relevant authors, Authors' production over time, Words frequency over time (authors keywords), Trend topics (keywords), Publication trends, Most relevant sources, The globally cited documents, Most cited countries, Countries' production over time, Tracing Collaboration Patterns. A bibliometric analysis of the data was carried out with visualization of the results. During this step, the following tools were used: Microsoft Excel v2407, Rstudio 2023.12.1 Build 402 and Biblioshiny 4.1.4. (Cobo et al., 2011; Donthu et al., 2021) for analysis, mapping and visualization of bibliometric data. Using Biblioshiny and Rstudio for bibliometric analysis has numerous advantages over other software alternatives. These tools offer a high degree of adaptability and flexibility, enable working with large amounts of data and integrating different data sources. Biblioshiny provides an intuitive interface for interactive visualizations, while Rstudio enables advanced data processing and creation of custom scripts. Both tools are free and supported by active communities, making them an economical choice compared to commercial software. In addition, they enable reproducible research and provide extensive opportunities for dynamic analyses, making them extremely useful for researchers.

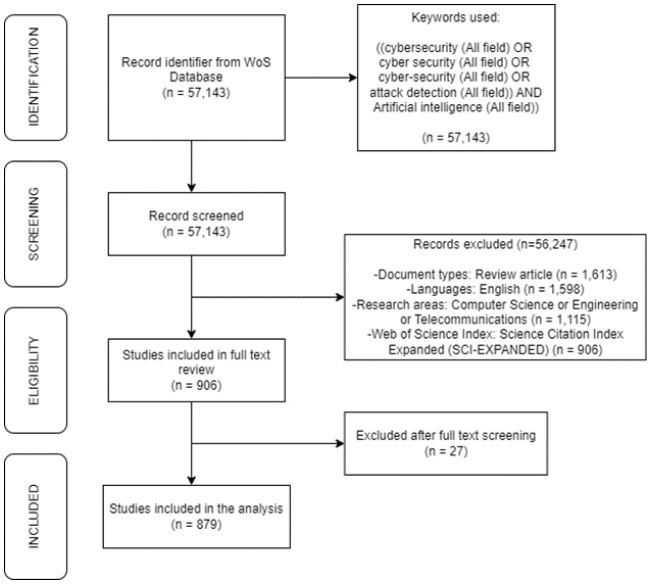

Figure 1. PRISMA flowchart
Source: Adapted from Page et al. (2021)

2.7. Review report writing

A report study was written and a discussion was held on the results of the research. In the discussion, we made a comparison with works dealing with the same research questions with different methodologies and in different databases. This methodological framework enables a systematic approach to the analysis of literature on the topic of artificial intelligence in cybersecurity, identifying key trends and research directions in this area.

3. Analysis

The impact of artificial intelligence in cybersecurity and attack detection is very significant in the IT industry (Ansari et al., 2022). The topic is relatively new and under researched, with even less industry discussion, so solutions for individuals facing problems in this area are rarely available. The next part of the paper will present the results, conduct content analysis through bibliometric analysis, adhering to the methodological steps described in the previous part. It is important to note that the subsections below are derived from the collected dataset for the given keywords. When referring to terms such as "Most relevant authors" or "Most relevant sources," these categories are based on the dataset's classifications. The terminology used in our analysis corresponds directly with the categories available in Biblioshiny, the tool employed for data extraction. Thus, readers can expect consistency between the categories discussed in this paper and those visible in Biblioshiny.

3.1. Most relevant authors

Based on the collected data on the number of articles published by the authors, as well as the fractional values that reflect the average number of citations per article, the following authors were highlighted:

- Kim-Kwang Raymond Choo (University of Texas at San Antonio, USA) leads in the number of published articles with 13, while its fractional value is 2.88
- Muhammad Ali Babar (University of Adelaide, Australia) and Tiago M. Fernández Caramés (Universidade da Coruña, Spain) share second place with nine published articles each and fractional values of 2.59 and 2.83.

- In third place are Junwei Zhang (School of Cyber Engineering, Xidian University, China) and Yang Wang (Concordia University. Montreal, QC, Canada), with 9 and 8 published articles each, and fractional values of 1.90 and 2.25.

Other notable authors include Yiming Zhang (Institute for Optimization and Decision Analytics, Liaoning Technical University, Fuxin, PR China), Ahmed Ali (College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia), Chuan Zhang (Southeast University – China), Paula Fraga-Lamas (Universidade da Coruña, Spain), and Mohammad Kamrul Hasan (National University of Malaysia), with varying numbers of published articles and fractional values further contributing to their profile in the research community. This review of authors provides insight into their contributions to the scientific literature, highlighting their productivity and impact, and you can see the data in the table shown below (Table 1).

Table 1. Most relevant authors

Authors	Articles	Articles fractionalized	H-index	Citations
Kim-Kwang Raymond Choo	13	2.88	89	22,204
Muhammad Ali Babar	9	2.59	35	3,228
Junwei Zhang	9	1.90	33	4,066
Yang Wang	8	2.25	46	11,033
Yiming Zhang	8	1.89	36	3,906
Ahmed Ali	6	1.07	15	347
Chuan Zhang	6	0.57	23	2,432
Tiago M. Fernández Caramés	6	2.83	33	2,895
Paula Fraga-Lamas	6	2.83	31	2,676
Mohammad Kamrul Hasan	6	0.89	27	1,858
Kim-Kwang Raymond Choo	13	2.88	89	22,204
Muhammad Ali Babar	9	2.59	35	3,228
Junwei Zhang	9	1.90	33	4,066
Yang Wang	8	2.25	46	11,033
Yiming Zhang	8	1.89	36	3,906

Source: Authors

3.2. Authors production over time

Authors were analyzed based on the number of publications per year, the total number of citations (TC), as well as the average number of citations per year (TCpY). The picture shows that some authors achieved a significant number of publications and citations during the observed period. For example, the author Ali A published 6 publications in total during 2020, 2021 and 2022, with a total of 85 citations, which gives an average of 6.5 citations per year. Another author, Babar Ma, was also very productive with 9 publications in the same period and a total of 242 citations, with an average of 10.2 citations per year. One of the most productive authors, Chen Z, has 6 publications and a total of 1739 citations during 2021 to 2023, with an average of 483.3 citations per year. These results show a high level of activity and influence of these authors in the research community. Further analysis shows that authors such as Choo Kkr and Fernandez-Carames Tm have also made a significant impact with their publications during the previous years, the data is shown in Figure 2.

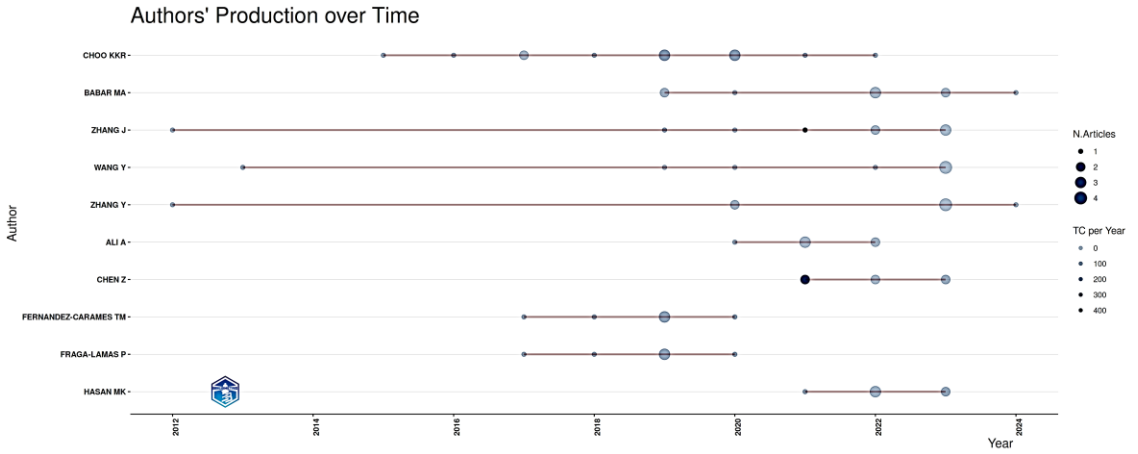

Figure 2. Authors production over time
Source: Authors

3.3. Words frequency over time (authors keywords)

As we can see in Figure 3, the results show a significant increase in the frequency of terms such as "cybersecurity", "security", "machine learning", "internet of things", "cyber security", "deep learning", "blockchain", "artificial intelligence", "IOT" and "privacy" during the observed period. For example, the term "cybersecurity" appears 164 times in 2024, compared to zero occurrences in 2004, which clearly indicates the increasing importance of this term in the modern information society. It should also be noted that the terms "cyber-security", "security" and "cyber security" can be viewed as one term that is written in several different ways, so the number of occurrences increases to 394 (164+153+77) in 2024. Of particular importance is the growing trend of terms such as "machine learning", "deep learning" and "artificial intelligence", which reflects the growing interest in the application of artificial intelligence in the field of cybersecurity. The number of citations for these terms has grown significantly over the past few years, reflecting researchers' efforts to use advanced machine learning techniques to more effectively protect information systems. Frequency analysis of these key terms provides insights into the main research topics in cybersecurity and artificial intelligence.

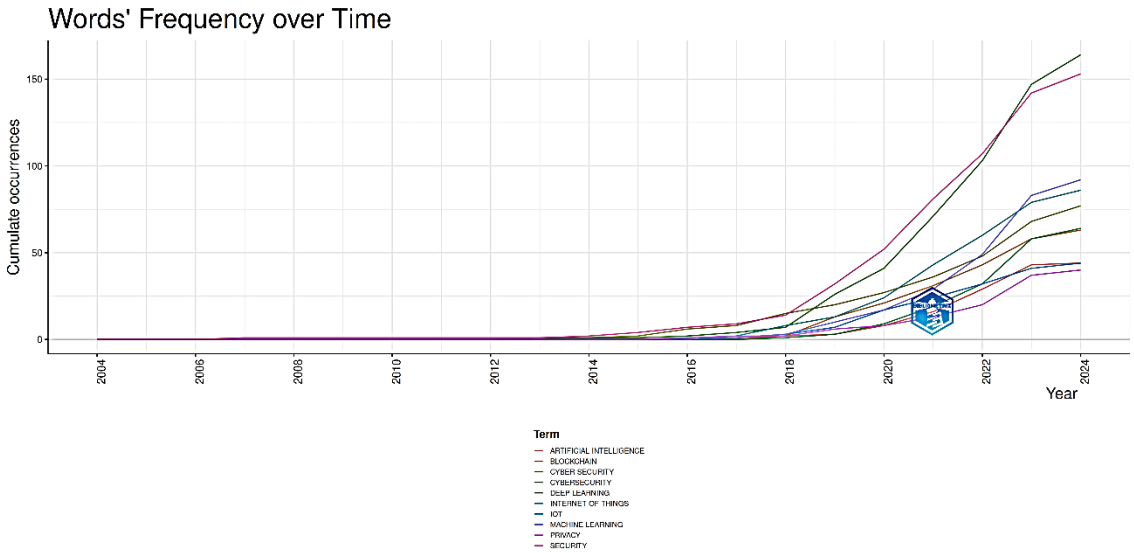

Figure 3. Keywords used by authors
Source: Authors

3.4. Trend topics (keywords)

As part of the research, key topics were identified that were the most frequent subject of research in the field of cybersecurity and artificial intelligence during the last few years. These topics not only reflect current research interests, but also provide insight into future research directions.

A review of the data from Figure 4 shows that the keywords "internet" (186 times), "security" (163 times) and "challenges" (129 times) are mentioned most often. These keywords have been particularly emphasized since 2020, with a median in 2022 and frequent mentions until 2023, indicating their continued relevance and relevance. "Privacy" (89 times) and "management" (73 times) are also prominent keywords that have become more prevalent in the literature since 2019 and 2020, with a median in 2021, highlighting the growing concern for protecting privacy and effectively governance in cyberspace. "Architecture" (55 times) and "cloud" (29 times) have stood out since 2020, reflecting the growing interest in the structural aspects of systems and cloud data processing and storage technologies. "Technologies" (30 times) and "information" (24 times) are frequently used keywords in scientific papers, with a focus on advanced technologies and information management from 2019 and 2020, indicating continuity and constant development in these areas. Keywords such as "blockchain" (27 times) and "intrusion detection system" (23 times) appear intensively only from 2022, with a median of 2023, suggesting an increasing interest in innovative approaches and technologies to improve cybersecurity. Also, "intelligence" (14 times) is a keyword that began to appear more significantly from 2022 (Liberati et al., 2009), indicating the growing role of artificial intelligence in the detection and prevention of cyber attacks. Other keywords such as "support" (8 times), "sensor networks" (6 times), "wireless" (5 times), and "power-systems" (6 times) are also important aspects of cybersecurity research, with different periods of intensity from 2016 to 2022. As part of the research, key topics were identified that were the most frequent subject of research in the field of cybersecurity and artificial intelligence during the last few years. These topics not only reflect current research interests, but also provide insight into future research directions.

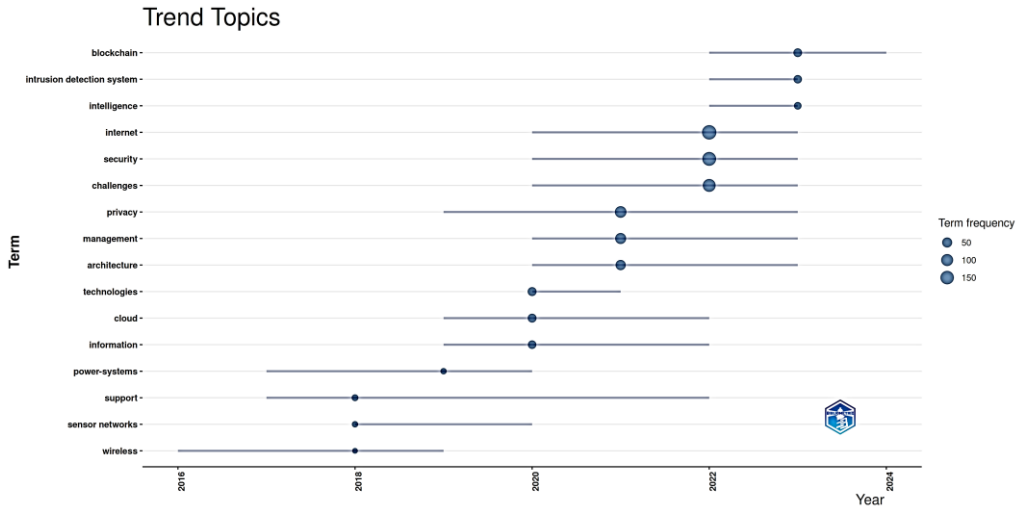

Figure 4. Trend topics – used keywords
Source: Authors

These trends in research papers provide a clear picture of the evolution of scholarly interests and focuses within cybersecurity, highlighting how technological advances and new threats are continuously shaping this dynamic field of research. Research trends show that topics such as the Internet, security and privacy are dominant, which reflects the current challenges in cybersecurity. The increased interest in artificial intelligence, especially in the context of attack detection, indicates its increasing importance and potential for improving security technologies.

3.5. Publication trends

By analyzing the annual trends in the publication of scientific papers in the field of cybersecurity, we can see that there has been a significant growth in recent years. We can notice in Figure 5 that starting with two articles in 2004, the publication of scientific papers experienced a significant increase during the past decade. The graph highlights the year 2023 with the largest number of published works of 213 articles, which emphasizes the accelerated development of research activities in this area. In the first half of 2024, the number of articles is already at 86. These data indicate a continued dynamic in the cybersecurity research community, where the annual production of articles increases as technological and societal challenges evolve.

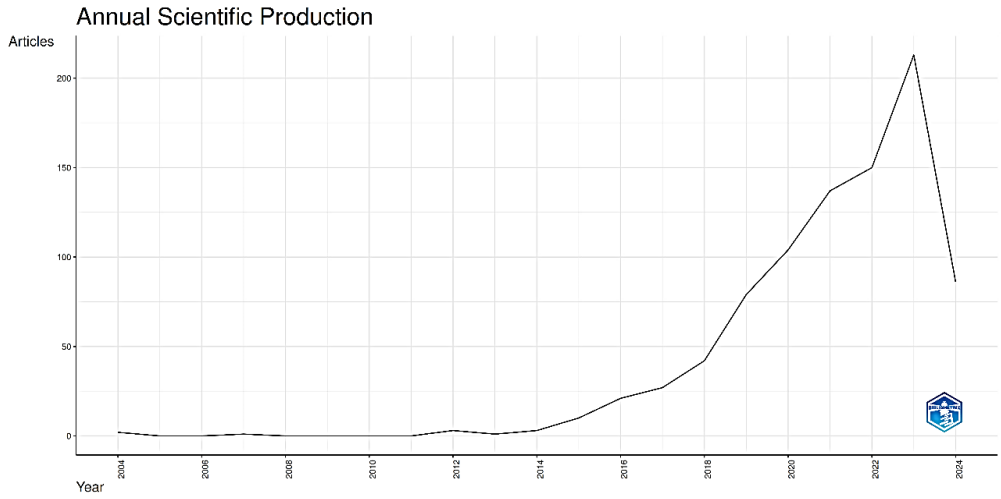

Figure 5. Publication trends
Source: Authors

3.6. Most relevant sources

Based on the number of published papers for each source found in Figure 6, we can identify key publications that have significantly contributed to the literature in this discipline. The most scientific papers were published in the IEEE Access journal with 110 papers, making it the most cited source. They are followed by the journals Sensors with 86 papers and Applied Sciences-Basel with 62 papers, which confirms their significant contribution. Also, notable sources such as Electronics, Computers & Security, and Computer Science Review are also among the most cited, with 53, 39, and 27 papers respectively. These results indicate a wide range of sources used in research, from general journals such as IEEE Access to specialized publications such as Sensors.

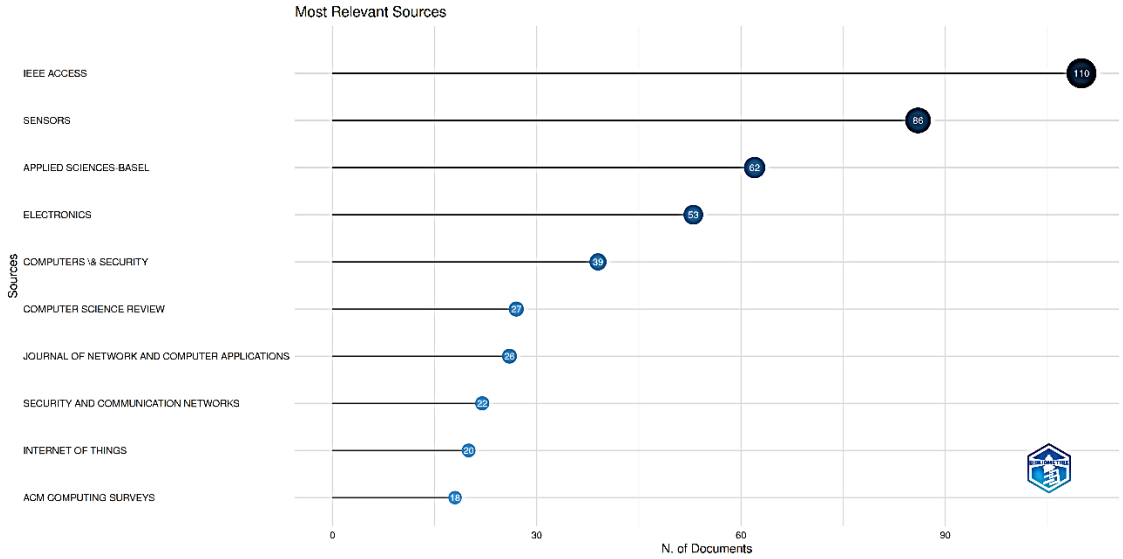

Figure 6. Most relevant sources
Source: Authors

3.7. The globally cited documents

The most cited papers come from various prestigious journals and cover a wide range of topics. They feature big data analysis, advanced methods, application of artificial intelligence, security challenges in network applications, smart grids, Internet of Things (IoT), and blockchain technology.

The results of the bibliometric analysis showed the ten most cited papers in the field of cybersecurity, with a focus on artificial intelligence and attack detection, which we can see in Table 2. These papers, published in various high-ranking journals, have contributed significantly to researchers and have become key resources for scholars around the world. of the world.

Table 2. The globally cited documents

Authors	Title	DOI	Total citations
Laith Alzubaidi et al.	Review of deep learning: concepts, CNN architectures, challenges, applications, future directions	10.1186/s40537-021-00444-8	1879
Xiaohu You et al.	Towards 6G wireless communication networks: vision, enabling	10.1007/s11432-020-2955-6	833

	technologies, and new paradigm shifts		
Md Zahangir Alom et al.	A State-of-the-Art Survey on Deep Learning Theory and Architectures	10.3390/electronics8030292	812
Mohiuddin Ahmed et al.	A survey of network anomaly detection techniques	10.1016/j.jnca.2015.11.016	679
Gaoqi Liang et al.	A Review of False Data Injection Attacks Against Modern Power Systems	10.1109/TSG.2015.2495133	541
Bruno Bogaz Zarpelão et al.	A survey of intrusion detection in Internet of Things	10.1016/j.jnca.2017.02.009	487
Khaled Salah et al.	Blockchain for AI: Review and Open Research Challenges	10.1109/ACCESS.2018.2890507	398
Anne H. Ngu et al.	IoT Middleware: A Survey on Issues and Enabling Technologies	10.1109/JIOT.2016.2615180	389
Thomas McGhin et al.	Blockchain in healthcare applications: Research challenges and opportunities	10.1016/j.jnca.2019.02.027	349
Francesca Meneghello et al.	IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices	10.1109/JIOT.2019.2935189	339

Source: Authors

These works are not only highly cited, but also very influential, providing the foundation for further research and development of new technologies in cybersecurity. The high number of citations received by these works testifies to their importance and influence on the scientific community. They represent a resource of crucial importance to researchers working to improve security systems and technologies. The growing number of these works and their citations show how urgent and important it is to develop new technologies for detecting and preventing cyber-attacks, as this is crucial for digital security.

3.8. Most cited countries

The data in Figure 7 is compiled based on the total number of citations (TC), author affiliation and average number of citations per paper for each country, which provides insight into their scientific productivity and impact in a global context. At the top of the list is the United States of America (USA) with 7392 citations and an average number of citations per paper of 64.80. Australia follows with 4610 citations and a high average number of 80.90 citations per paper. China and India also show significant influence, with 3686 and 2587 citations respectively, while the average number of citations per paper is somewhat lower. We single out countries such as the United Kingdom, Italy, the United Arab Emirates, Brazil, and Lebanon, which also achieve high productivity and influence in the field of publishing scientific works. These results emphasize the global character of research, as well as the importance that individual countries have in the generation of knowledge and progress in this discipline.

Further analysis of these data can provide deeper insight into the factors that contribute to the scientific productivity and impact of countries around the world.

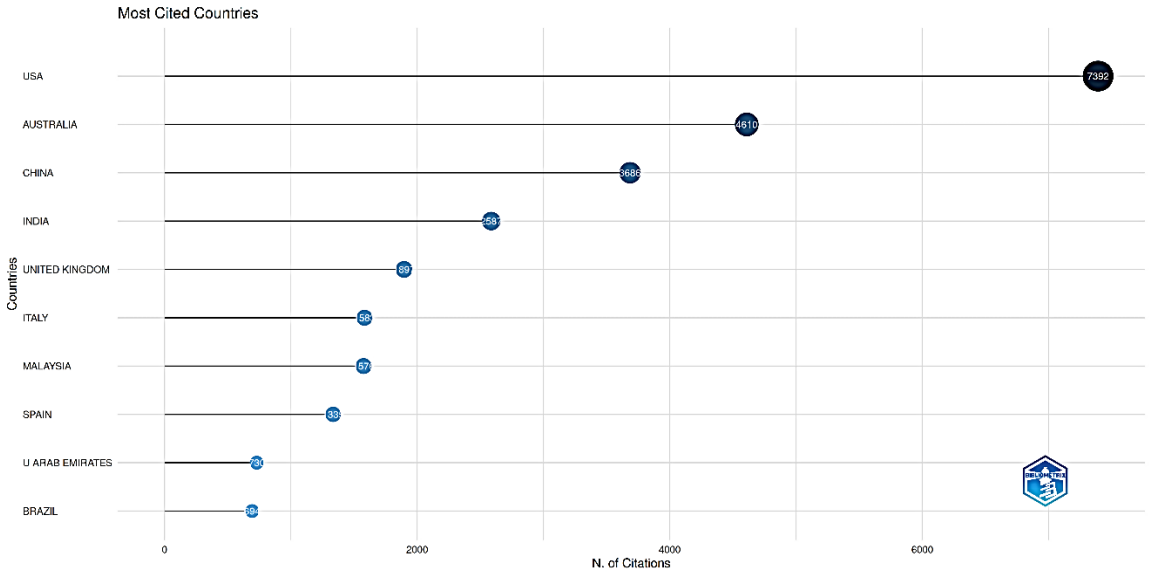

Figure 7. Most cited countries
Source: Authors

3.9. Countries production over time

The analyzed data from Figure 8 are about scientific works in different countries during the last twenty years. These data provide insight into global trends and research progress in the field of cybersecurity with a special emphasis on the application of artificial intelligence.

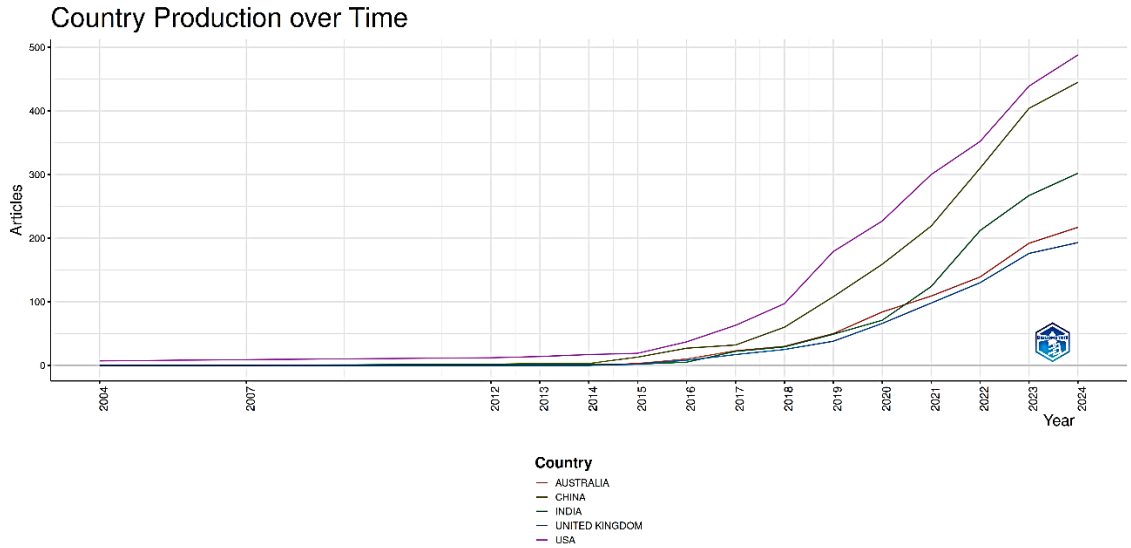

Figure 8. Countries production over time
Source: Authors

The United States of America (USA) leads the way in the production of scientific papers in the field of cybersecurity. Since 2004, when only seven articles were recorded, the number of published works is increasing, 488 articles in 2024. This trend highlights the continued commitment and significant investment in research and development in this area, especially in the last decade.

China records similar growth, but with a slightly later start of intensive research (Zhu & Liu, 2020a). Until 2012, China had only a few published papers, but since then the number of articles has increased drastically, reaching 445 in 2024. These data suggest an accelerated development of research capacities and an increasing interest in cybersecurity and artificial intelligence.

We should not ignore India and Australia, which also show significant growth in the publication of scientific works in this field. India began publishing papers around 2012, while Australia recorded its first significant results a few years later. Both countries have recorded a significant increase in the number of articles since the middle of the second decade of the 21st century, which indicates an increasing commitment and capacity in the field of cybersecurity research.

The United Kingdom follows a similar pattern, with a slower start but accelerated growth in the last decade. Starting from zero in 2004, the number of papers published in the UK is expected to rise to 193 in 2024, reflecting increased activity and interest in this area of research.

These results indicate a global trend of growth in research related to cybersecurity and artificial intelligence, with the US as the leader, while other countries, such as China, India, Australia and the United Kingdom, are significantly increasing their efforts, resources and capacities in this area. A growing number of scientific papers show how important it is to develop new technologies to detect and prevent cyber-attacks, as this is key to security in the digital world. Centrally managed systems, which are often pivotal to organizational infrastructure, are particularly vulnerable to illegal exploitation and cybercrime attacks, highlighting the urgency for advanced solutions in cybersecurity (Yazdinejad et al., 2020).

3.10. Tracing collaboration patterns

By analyzing Figure 9, Tracing collaboration patterns, we can see cooperation between countries in the field of cybersecurity reveals several key trends. By using different metrics, such as Betweenness, Closeness and PageRank, we can identify countries that are central to the global research collaboration network.

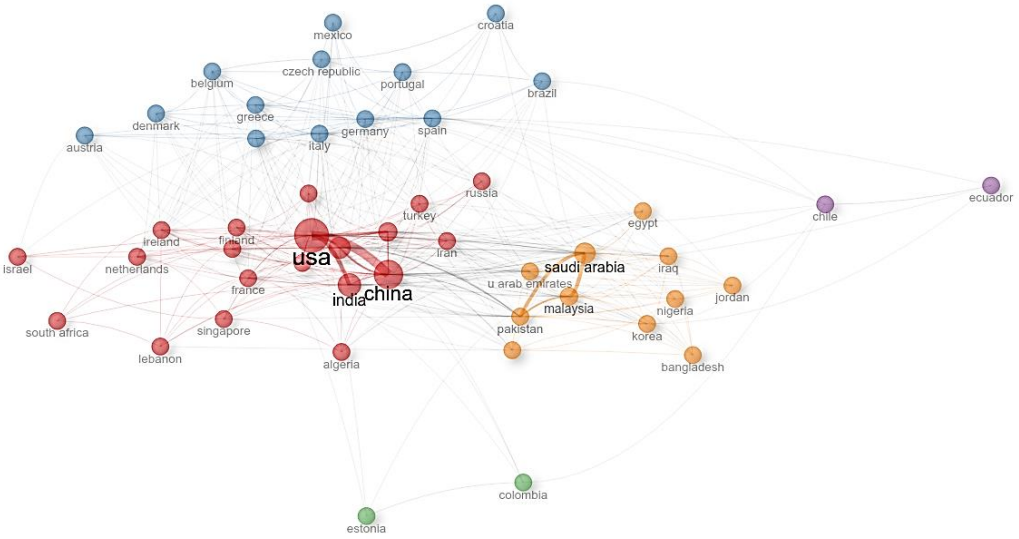

Figure 9. Tracing collaboration patterns
Source: Authors

The United States of America (USA) dominates with the highest values of Betweenness (244.88), Closeness (0.0192) and PageRank (0.0940), which indicates its central role in connecting

and spreading research activities around the world. China and India, also from cluster 1, follow with significant but lower values compared to the USA, confirming their growing importance in the global research network. European countries, such as the United Kingdom, France, Sweden and others, also play significant roles within the same cluster, with solid Betweenness and Closeness values. Italy, Spain, and Germany, belonging to cluster 2, also show high values, highlighting their role in European cooperation. Saudi Arabia and Malaysia, from cluster 5, stand out with high Betweenness and PageRank values, which indicates their significant influence and connection within their group, as well as with the rest of the world. Research trends show that topics such as the Internet, security and privacy are dominant, which reflects the current challenges in cybersecurity. The increased interest in artificial intelligence, especially in the context of attack detection, indicates its increasing importance and potential for improving security technologies.

These patterns of cooperation show that some countries play a key role in the global research network, but there are also regional centers that are also important in their own groups. These centers not only facilitate cooperation in their regions, but also connect their communities with global research flows. They thereby contribute to the development of cybersecurity on a global level.

4. Discussion

In this paper, a detailed analysis of the current state of research in the field of artificial intelligence and cybersecurity was carried out, with a special focus on attack detection. Through bibliometric analysis, the most relevant authors, key topics, publishing trends, as well as global patterns of collaboration were investigated. The analysis showed that authors such as Choo Kkr, Babar Ma, and Fernandez-Carames Tm are among the leaders in the number of published papers and fractional values, which indicates their significant contribution in this field. Their activity and influence during the observed period suggest that these authors have significantly contributed to the progress in cybersecurity research. The research (Sharma et al., 2023), which was done in 2023, is shown: 10 most productive authors in the field cybersecurity and forensic, shows the authors differently, which is normal, considering that our research is narrowly focused and partly different from the work we analyzed and compared and if both works were aimed at security in cyber space. Another paper (Mukherjee & Barui, 2023) used the same bibliometric analysis, but the results were different in that paper as well as the search strategy and keywords were different. This only shows how much works with the same topic and the same method of processing can differ and that each work is unique in its own way and brings new light on the subject in scientific circles.

The frequency of keywords such as "cybersecurity", "machine learning", "deep learning" and "artificial intelligence" has seen a significant increase in the last few years, which indicates a growing interest in the application of advanced machine learning and artificial intelligence techniques in the field of cybersecurity. And in other researches (Ahmed et al., 2022; Sharma et al., 2023; Yazdinejad et al., 2020; Zhu & Liu, 2020a) it is similar when looking at cybersecurity in combination with AI with small deviations that are understandable if you look at the search strategy and the database that the authors searched. Thematically, the research is dominated by terms such as "internet", "security" and "challenges", while terms such as "blockchain" and "intrusion detection system" have become popular only recently. The thematic presentation of the research is not so common in the work (Albahri & AlAmoodi, 2023) that we compared, and it is largely different from our research. This can be justified by the fact that the mentioned research used a different database and that for this reason the data are quite different. This reflects current challenges and interests in cybersecurity. The number of published works in the

field of cybersecurity is growing significantly, with a peak in 2023. This is the same or similar to other research conducted in the last few years (Albahri & AlAmoodi, 2023; Ivanova et al., 2024; Mukherjee & Barui, 2023; Sharma et al., 2023). This indicates the accelerated development of research activities and the growing attention paid to this area. Key sources for publications include journals such as IEEE Access, Sensors and Applied Sciences-Basel, which provide a platform for publishing high quality research papers. Research from 2023 (Sharma et al., 2023) records similar results for the first two papers, while in the following journals there is a difference, but it should be taken into account that the papers from the Scopus database were analyzed in this paper. Highly cited papers covering a wide range of topics from artificial intelligence to blockchain technology provide the foundations for further research and development in cybersecurity. The United States of America, Australia, China and India stood out as the leading countries in terms of the number of citations, which indicates their significant contribution and influence in the global research community. Those countries have also shown continued growth in the production of scientific papers, highlighting their commitment to cybersecurity research. It is interesting that the researches (Albahri & AlAmoodi, 2023; Ivanova et al., 2024; Mukherjee & Barui, 2023; Sharma et al., 2023) that we compared had mostly different results in the order of countries, but the same countries are constantly repeated, which proves their commitment to this topic, and therefore can show the trends that are expected in in the following years.

Collaboration Patterns show that the USA, China and India are central countries in the global research collaboration network, while European countries and regional centers also play significant roles in facilitating collaboration and knowledge exchange. The research (Ivanova et al., 2024), which was done on the WoS database as well as on Scopus, shows a much more developed network of cooperation in the Scopus database, while the cooperation in the WoS database is approximately similar to our pattern. These findings provide clear insight into current trends, key players and research priorities in the field of artificial intelligence and cybersecurity.

The growth in the number of publications and citations, as well as the increasing interest in advanced techniques such as machine learning and blockchain technology, indicate that these areas will continue to be the focus of future research. Increased cooperation between countries and institutions around the world will further contribute to the acceleration of the development of new technologies and methods for improving cybersecurity. Based on these findings, it is clear that research in this area is dynamic and rapidly evolving, and it is necessary to continue investing in research and development in order to effectively respond to increasingly complex threats in the digital world.

5. Conclusion

This paper presents a comprehensive overview of global trends and achievements in cybersecurity and artificial intelligence research, highlighting key aspects that shape contemporary science. The United States of America, as leaders in the publication of scientific works, sets standards in the development of new technologies for the protection of information systems and actively contributes to international cooperation and knowledge exchange. We must note that China, India and European countries are demonstrating their ability to cope with increasingly complex challenges in the digital environment, developing innovative approaches and technological solutions that improve global cybersecurity. These efforts not only strengthen local capacities but also improve the global security of digital systems, making them more resilient to increasingly sophisticated threats.

The development and application of advanced technologies such as artificial intelligence, blockchain and cloud computing technologies are key to future advancements in cybersecurity. This paper emphasizes the importance of further research and development of strategies that will respond to increasing challenges in the digital space, ensuring the stability and integrity of information systems around the world.

We conclude that the growing interest in advanced techniques and increasing international cooperation will contribute to further progress in the development of effective methods to protect against cyber threats. Continued research and investment in this area is critical to maintaining security in an increasingly complex digital environment.

5.1. Limitations and future research

This study exclusively uses the Web of Science (WoS) database, which is one of the leading and respected sources in the field of scientific research. Bibliometric analysis, as a method, allows for a quantitative evaluation of scientific production, and WoS is an appropriate choice as it covers the most relevant and highly cited scientific papers, providing a thorough insight into global research trends. However, it represents only one aspect of the available resources. In future research, while this study remains focused on WoS to maintain its methodological consistency, it would be beneficial to extend the analysis by including other databases, such as Scopus, Google Scholar, or other relevant sources. This approach would avoid the need to rework the current study from the beginning and instead, build upon it by broadening the scope in subsequent research. This would provide a more complete insight into the research area and contribute to a more comprehensive analysis. Moreover, although the number of citations can indicate the visibility and recognition of works in the scientific community, this measure is not always indicative of the quality of research. Early papers may be highly cited because they represent foundational theories or discoveries, but this does not necessarily guarantee high quality or relevance. Additionally, certain fields may have a tendency to cite more papers within their discipline, which can skew citation counts. These potential biases underline the importance of combining citation metrics with other indicators, such as peer reviews or practical applications, to obtain a more balanced and accurate assessment of a paper's value. Addressing these limitations in future works can lead to more precise and comprehensive results that better illuminate the researched topic.

References

Ahmed, S., Alshater, M. M., Ammari, A. E., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. Research in International Business and Finance, 61, 101646.

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

Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. International Journal of Computer (IJC), 24(1), 100–116.

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. Legal Issues in the Digital Age, 2, 78–121.

Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: A literature review. International Journal of Advanced Research in Computer and Communication Engineering.

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. International Journal of Social Research Methodology, 8, 19–32.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54, 3849–3886.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly, 35, 1017–1041.

Bieniasz, J., & Szczypiorski, K. (2021). Dataset generation for development of multi-node cyber threat detection systems. Electronics, 10(21), 2711.

Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. In Effective Model-Based Systems Engineering (pp. 345–404). Springer.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv. https://arxiv.org/abs/1802.07228

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools. Journal of the American Society for Information Science and Technology, 62, 1382–1402.

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57–106.

Deng, L., & Liu, Y. (2018). A joint introduction to natural language processing and to deep learning. In Deep Learning in Natural Language Processing (pp. 1–22). Springer.

Dissanayake, M. B. (2021). Feature engineering for cyber-attack detection in Internet of Things. International Journal of Wireless and Microwave Technologies, 11(6), 46–54.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285–296.

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning algorithms for anomaly detection. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1–8). IEEE.

Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained IoT networks. Distributed Learning and Broad Applications in Scientific Research, 5, 23–54.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094.

Gupta, C., Johri, I., Srinivasan, K., Hu, Y. C., Qaisar, S. M., & Huang, K. Y. (2022). A systematic review on machine learning and deep learning models for electronic information security in mobile networks. Sensors, 22, 2017.

Hassani, H., Huang, X., & Silva, E. (2021). The human digitalisation journey: Technology first at the expense of humans? Information, 12, 267.

Hassani, H., Silva, E. S., Unger, S., TajMazinani, M., & Mac Feely, S. (2020). Artificial intelligence (AI) or intelligence augmentation (IA): What is the future? AI, 1, 8.

Ilić, L., Šijan, A., Predić, B., Viduka, D., & Karabašević, D. (2024). Research trends in artificial intelligence and security—Bibliometric analysis. Electronics, 13, 2288. https://doi.org/10.3390/electronics13122288

Ivanova, M., Grosseck, G., & Holotescu, C. (2024). Unveiling insights: A bibliometric analysis of artificial intelligence in teaching. Informatics, 11, 10. https://doi.org/10.3390/informatics11010010

Kitchenham, B. A., Mendes, E., & Travassos, G. H. (2007). Cross versus within-company cost estimation studies: A systematic review. IEEE Transactions on Software Engineering, 5, 316–329.

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: Revolutionizing cyber security in the digital era. Journal of Computers, Mechanical and Management, 2(3). https://doi.org/10.57159/gadl.jcmm.2.3.23064

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. Annals of Internal Medicine, 151(4), W-65. https://doi.org/10.7326/0003-4819-151-4-200908180-00136

Liu, W. (2019). The data source of this study is Web of Science Core Collection? Not enough. Scientometrics, 121, 1815–1824.

Makridakis, S. (2017). The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. Futures, 90, 46–60.

Masic, I. (2016). Index factors for assessing the scientific journal validity, its articles and their authors. Journal of Forensic Anthropology, 1(103), 2.

McBurney, M. K., & Novak, P. L. (2002). What is bibliometrics and why should you care? In Proceedings of the IEEE International Professional Communication Conference (pp. 108–114). IEEE.

Mukherjee, D., & Barui, S. K. (2023). Artificial Intelligence (AI) based cyber security solution during the period of 2013–2022: A bibliometric study. College Libraries, 38(IV), 90–102.

Mylrea, M., & Robinson, N. (2023). Artificial Intelligence (AI) trust framework and maturity model: Applying an entropy lens to improve security, privacy, and ethical AI. Entropy, 25(10), 1473.

Nadella, G. S., & Gonaygunta, H. (2024). Enhancing cybersecurity with artificial intelligence: Predictive techniques and challenges in the age of IoT. International Journal of Science and Engineering Applications, 13(4), 30–33.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). Updating guidance for reporting systematic reviews: Development of the PRISMA 2020 statement. Journal of Clinical Epidemiology, 134, 103–112. https://doi.org/10.1016/j.jclinepi.2021.02.003

Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cyber security trends, emerging technologies and threats. In R. Agrawal, J. He, E. Shubhakar Pilli, & S. Kumar (Eds.), Cyber security in intelligent computing and communications (Studies in Computational Intelligence, Vol. 1007). Springer. https://doi.org/10.1007/978-981-16-8012-0_2

Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of Scientific Research and Management, 9(12), 669–710.

Pessin, V. Z., Yamane, L. H., & Siman, R. R. (2022). Smart bibliometrics: An integrated method of science mapping and bibliometric analysis. Scientometrics, 127, 3695–3718.

Popkova, E. G., De Bernardi, P., Tyurina, Y. G., & Sergi, B. S. (2022). A theory of digital technology advancement to address the grand challenges of sustainable development. Technology in Society, 68, 101831.

Qiu, S., Liu, Q., Zhou, S., & Wu, C. (2019). Review of artificial intelligence adversarial attack and defense technologies. Applied Sciences, 9(5), 909.

Salih, A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC) (pp. 61–66). IEEE.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: A literature survey. Procedia Computer Science, 189, 19–28.

Sarker, I. H. (2024). AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability. Springer Nature.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2, 173.

Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. Journal of Engineering, 2020, 5267564.

Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. Revista Española de Documentación Científica, 15(4), 42–66.

Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. Results in Control and Optimization, 10, 100197.

Singh, A., Vaish, A., & Keserwani, P. K. (2014). Information security: Components and techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4(1).

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9, 1864.

Spremić, M., & Šimunić, A. (2018). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering 2018 (Vol. I). WCE 2018, July 4–6, 2018, London, U.K.

Yazdinejad, A., Dehghantanha, A., Srivastava, G., Karimipour, H., & Parizi, R. M. (2024). Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things. Journal of Systems Architecture, 148, 103088. https://doi.org/10.1016/j.sysarc.2024.103088

Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., & Choo, K.-K. R. (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Transactions on Services Computing, 13(4), 625–638. https://doi.org/10.1109/TSC.2020.2966970

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. IEEE Access, 9, 94318–94337.

Zhu, J., & Liu, W. (2020a). Comparing like with like: China ranks first in SCI-indexed research articles since 2018. Scientometrics, 124, 1691–1700. https://doi.org/10.1007/s11192-020-03525-2

Zhu, J., & Liu, W. (2020b). A tale of two databases: The use of Web of Science and Scopus in academic papers. Scientometrics, 123(1), 321–335.